FIG. 1

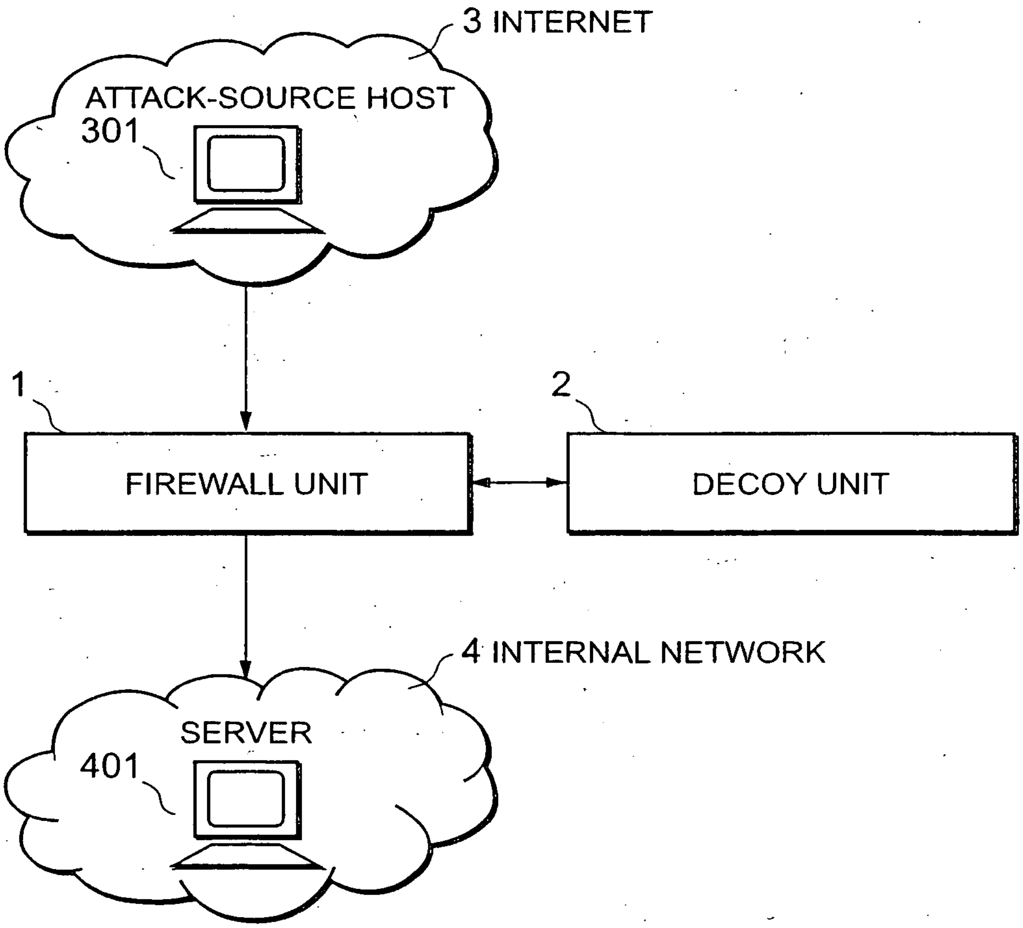

3 INTERNET
ATTACK-SOURCE HOST
301
1
FIREWALL UNIT
2
DECOY UNIT
4 INTERNAL NETWORK
SERVER
401

FIG. 2

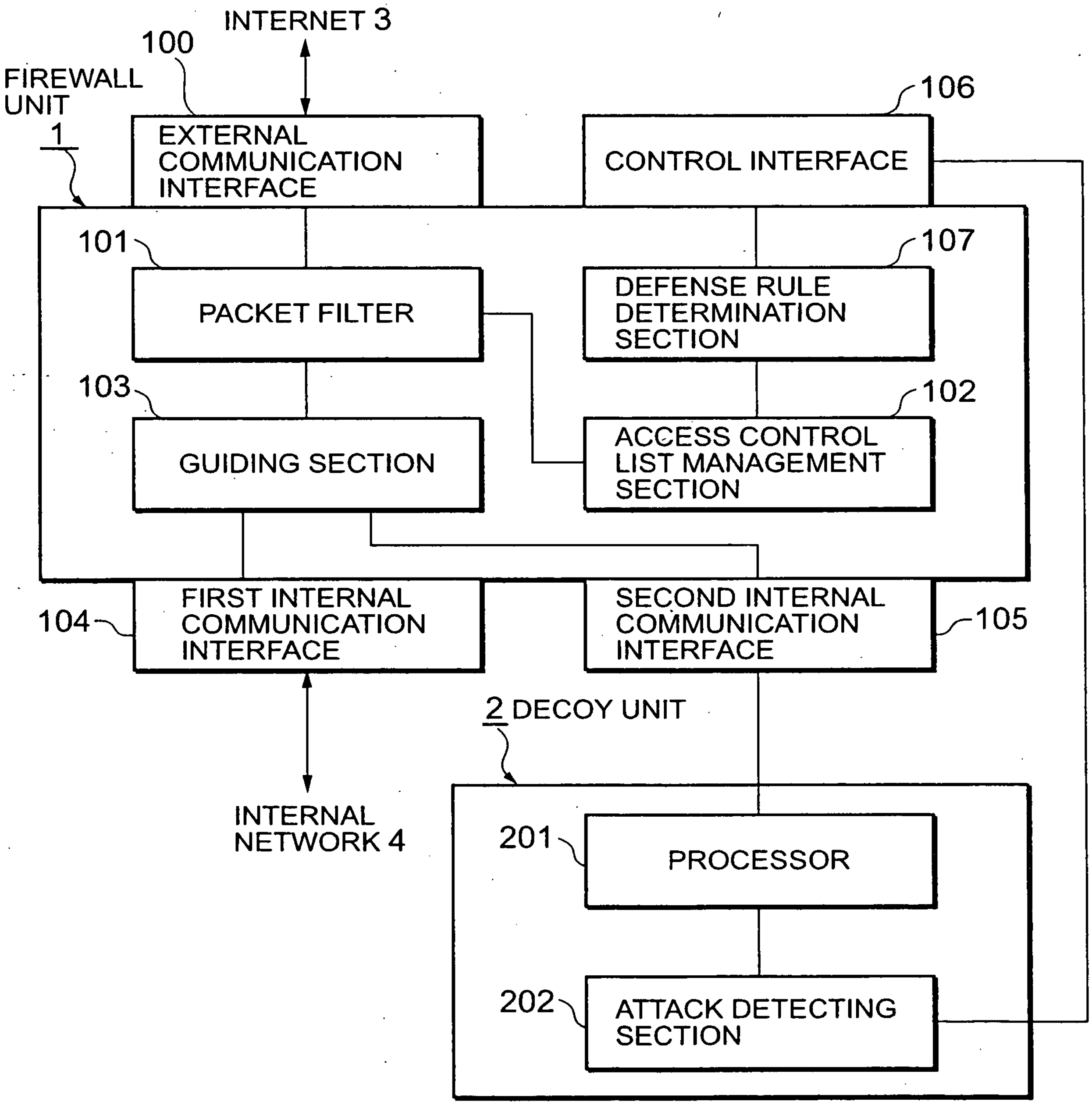

INTERNET 3
100
FIREWALL UNIT
1
EXTERNAL COMMUNICATION INTERFACE
106
CONTROL INTERFACE
101
PACKET FILTER
107
DEFENSE RULE DETERMINATION SECTION
103
GUIDING SECTION
102
ACCESS CONTROL LIST MANAGEMENT SECTION
104
FIRST INTERNAL COMMUNICATION INTERFACE
SECOND INTERNAL COMMUNICATION INTERFACE
105
2 DECOY UNIT
INTERNAL NETWORK 4
201
PROCESSOR
202
ATTACK DETECTING SECTION

FIG. 3

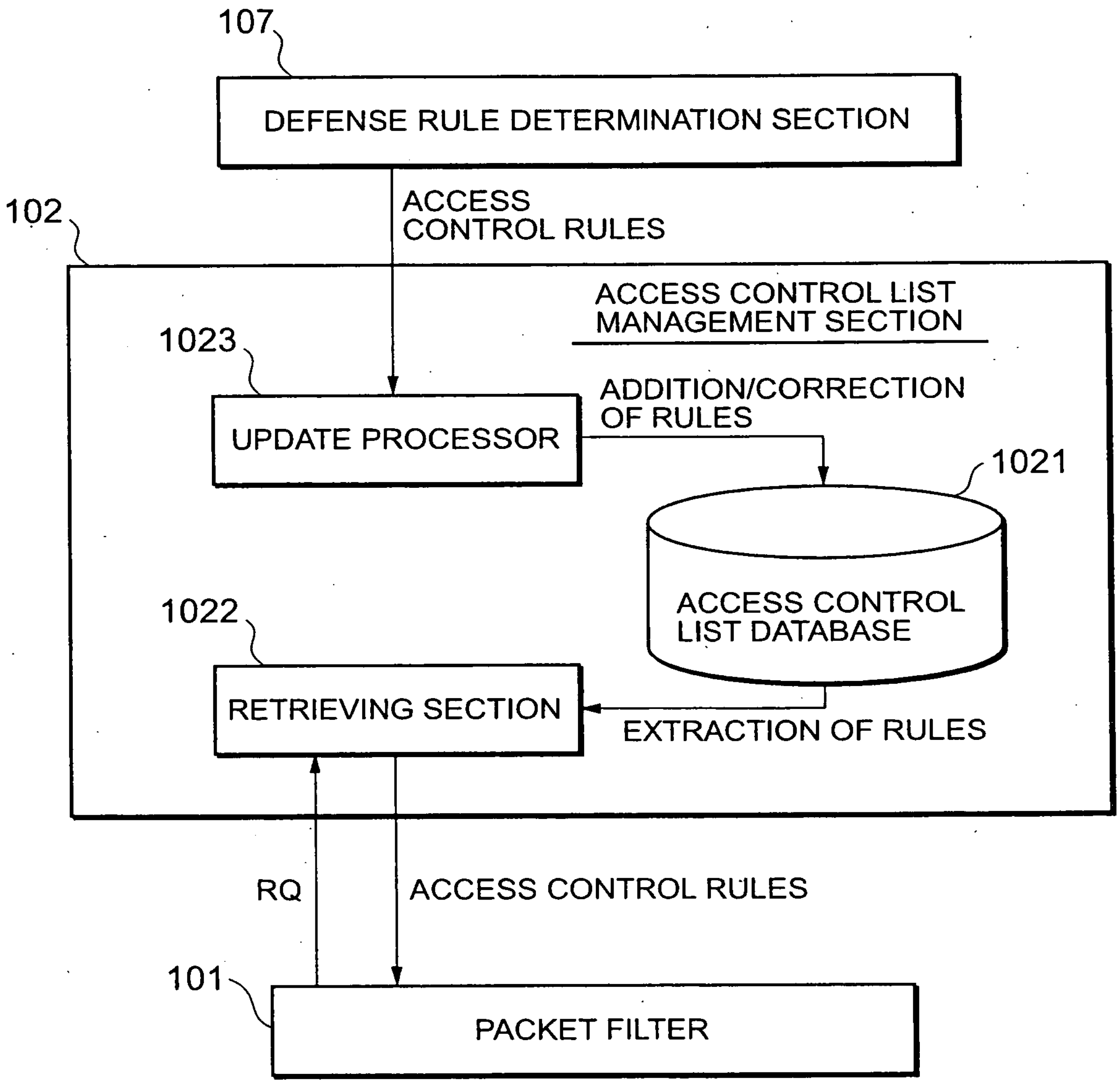

107
DEFENSE RULE DETERMINATION SECTION
ACCESS CONTROL RULES
102
ACCESS CONTROL LIST MANAGEMENT SECTION
1023
UPDATE PROCESSOR
ADDITION/CORRECTION OF RULES
1021
ACCESS CONTROL LIST DATABASE
1022
RETRIEVING SECTION
EXTRACTION OF RULES
RQ
ACCESS CONTROL RULES
101
PACKET FILTER

FIG. 4

1021

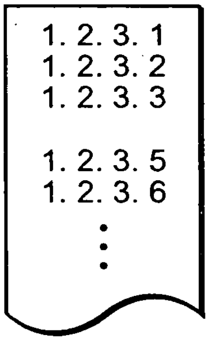
ACCESS CONTROL LIST DATABASE

SOURCE IP ADDRESS (SRC)	DESTINATION IP ADDRESS (DST)	PACKET FILTERING PROCESS (PROC)
*	1.2.3.1	ACCEPT
*	1.2.3.2	ACCEPT
12.34.1.1	*	ACCEPT
*	1.2.3.3	DROP
*	*	DENY

* : MATCHED WITH ARBITRARY ADDRESS
ACCEPT : ACCEPTANCE OF PACKET
DENY : DENIAL OF PACKET (WITH ICMP ERROR NOTIFICATION)
DROP : DROPPING OF PACKET (WITHOUT ICMP ERROR NOTIFICATION)

FIG. 5

GUIDING LIST



1. 2. 3. 1
1. 2. 3. 2
1. 2. 3. 3

1. 2. 3. 5
1. 2. 3. 6
⋮

FIG. 6

107

DEFENSE RULE DETERMINATION SECTION

ATTACK TYPE	SOURCE IP ADDRESS (SRC)	DESTINATION IP ADDRESS (DST)	PACKET FILTERING PROCESS (PROC)
RECON	—	—	—
INTRUSION	${SRC_IP_ADDRESS}	*	DROP
DESTRUCTION	${SRC_IP_ADDRESS}	*	DROP

- : WITHOUT ANY ADDRESS (NO PROCESSING)
${} : VARIABLE TO BE REPLACED

FIG. 7

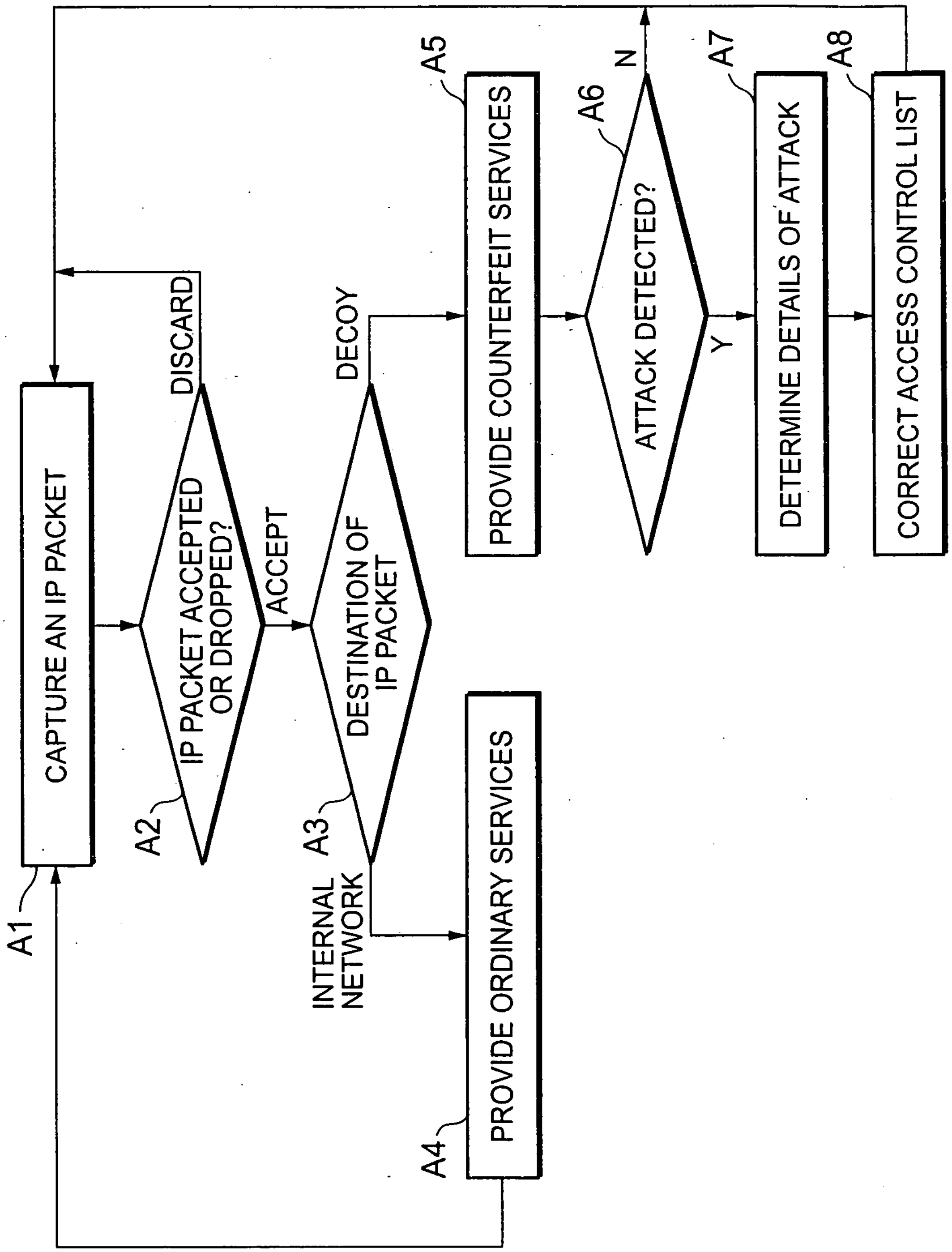

A1
CAPTURE AN IP PACKET
A2
IP PACKET ACCEPTED OR DROPPED?
DISCARD
ACCEPT
A3
DESTINATION OF IP PACKET
DECOY
INTERNAL NETWORK
A4
PROVIDE ORDINARY SERVICES
A5
PROVIDE COUNTERFEIT SERVICES
A6
ATTACK DETECTED?
N
Y
A7
DETERMINE DETAILS OF ATTACK
A8
CORRECT ACCESS CONTROL LIST

FIG. 8

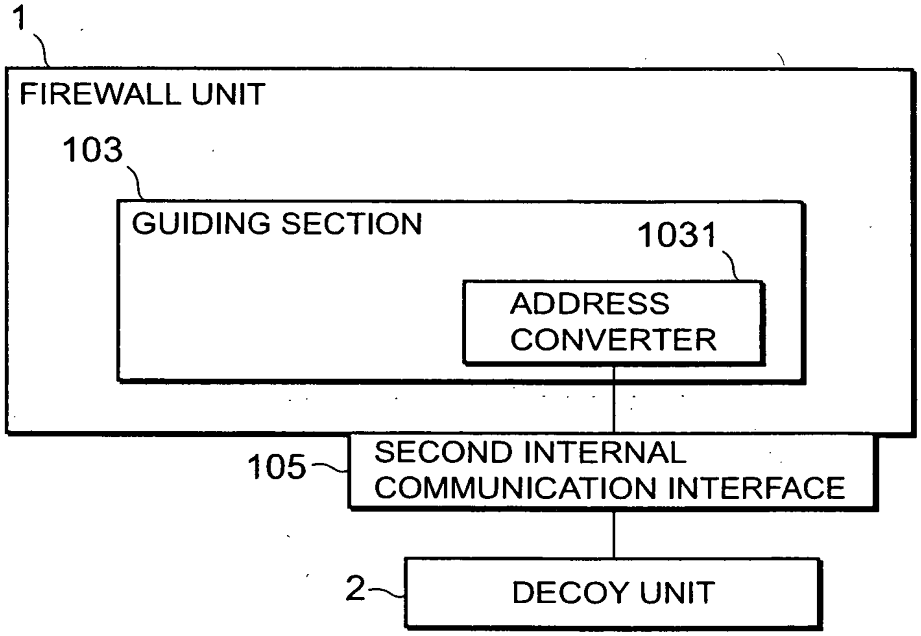

1
FIREWALL UNIT
103
GUIDING SECTION
1031
ADDRESS CONVERTER
105
SECOND INTERNAL COMMUNICATION INTERFACE
2
DECOY UNIT

FIG. 9

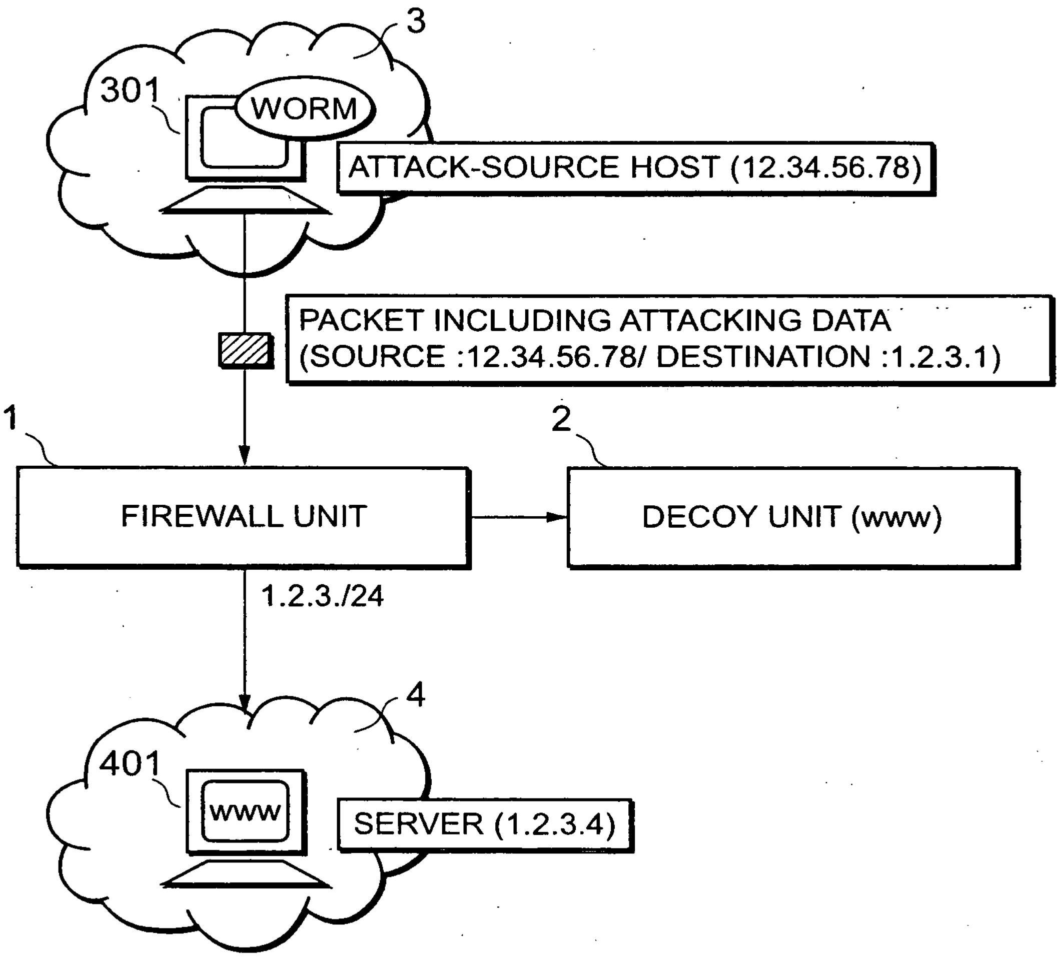

3
301
WORM
ATTACK-SOURCE HOST (12.34.56.78)
PACKET INCLUDING ATTACKING DATA
(SOURCE :12.34.56.78/ DESTINATION :1.2.3.1)
1
2
FIREWALL UNIT
DECOY UNIT (www)
1.2.3./24
4
401
www
SERVER (1.2.3.4)

FIG. 10

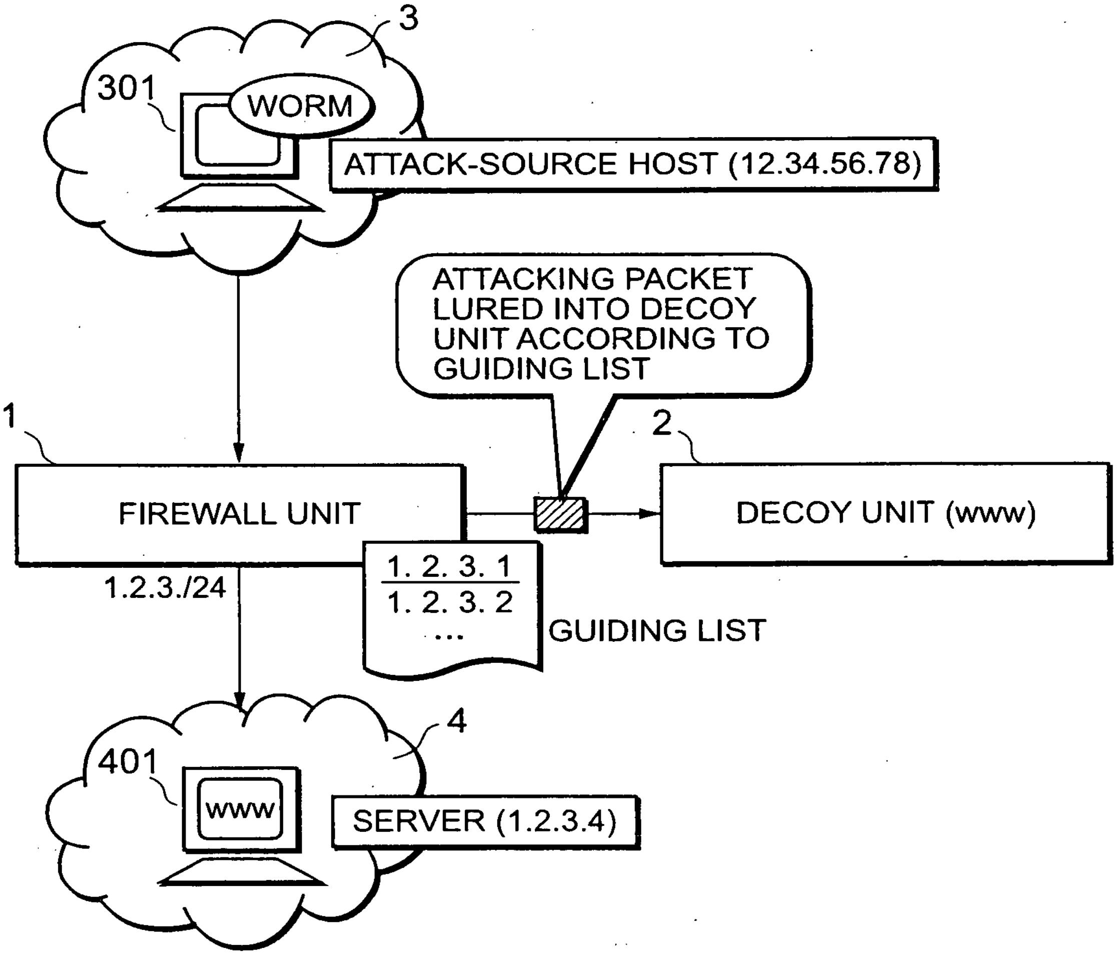

3
301
WORM
ATTACK-SOURCE HOST (12.34.56.78)
ATTACKING PACKET LURED INTO DECOY UNIT ACCORDING TO GUIDING LIST
1
FIREWALL UNIT
2
DECOY UNIT (www)
1.2.3./24
1. 2. 3. 1
1. 2. 3. 2
...
GUIDING LIST
4
401
www
SERVER (1.2.3.4)

FIG. 11

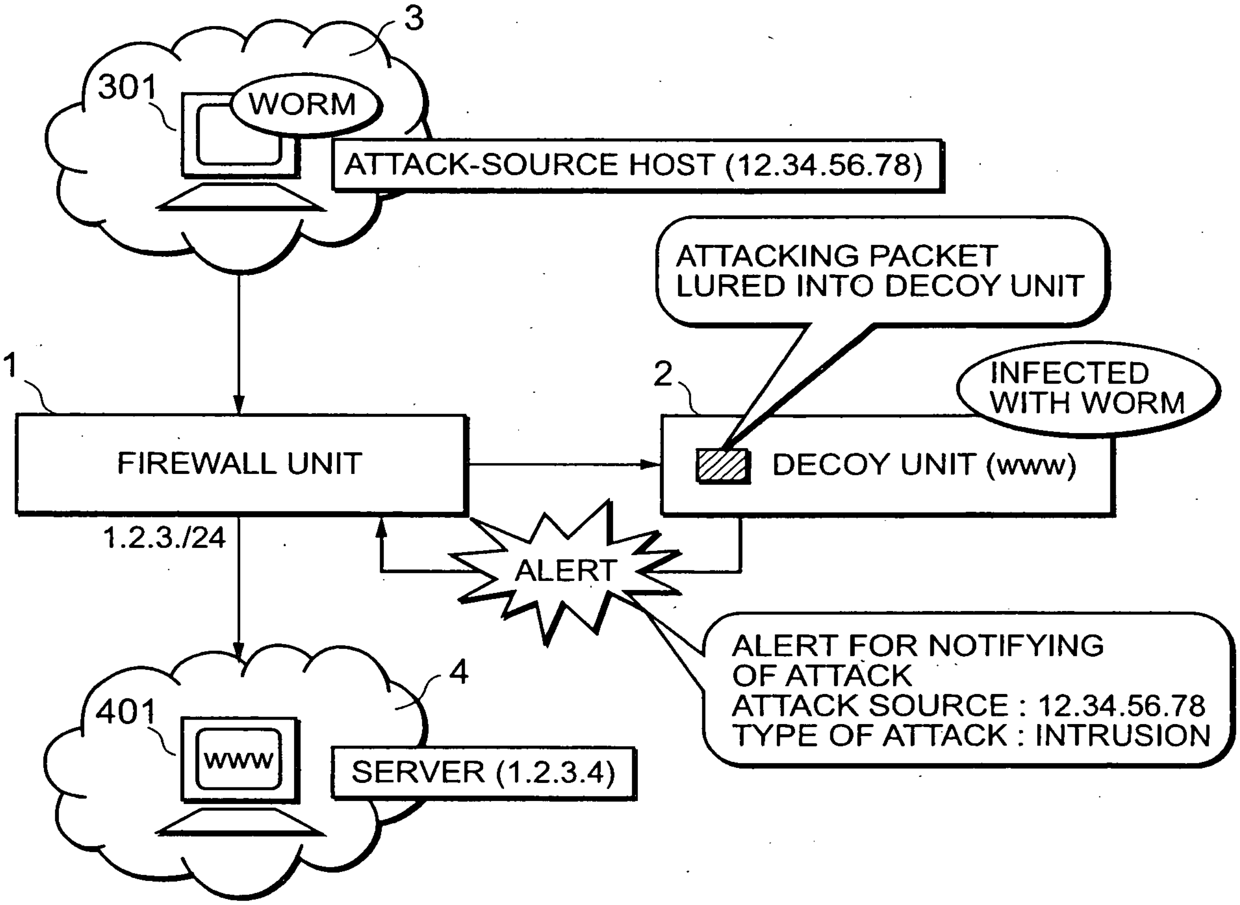
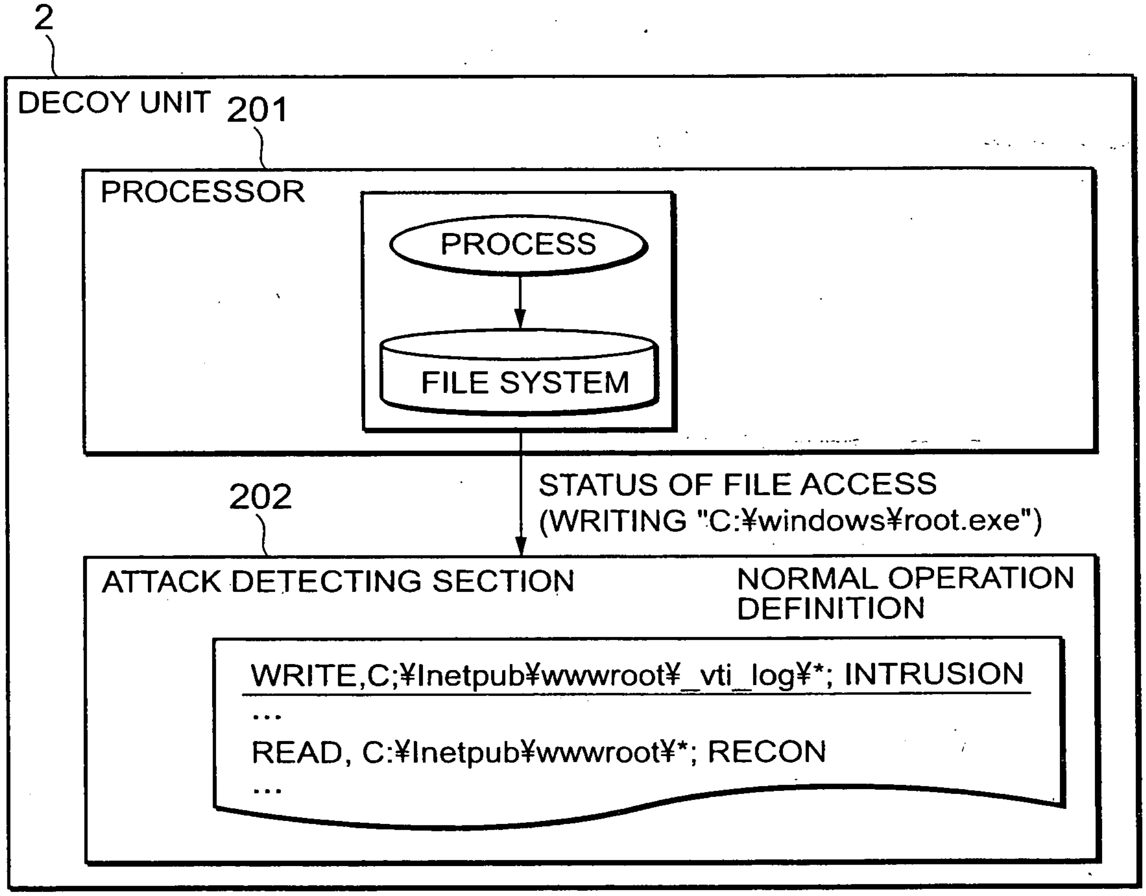

3
301
WORM
ATTACK-SOURCE HOST (12.34.56.78)
ATTACKING PACKET LURED INTO DECOY UNIT
INFECTED WITH WORM
1
FIREWALL UNIT
2
DECOY UNIT (www)
1.2.3./24
ALERT
ALERT FOR NOTIFYING OF ATTACK
ATTACK SOURCE : 12.34.56.78
TYPE OF ATTACK : INTRUSION
4
401
www
SERVER (1.2.3.4)

FIG. 12



```
WRITE,C;¥Inetpub¥wwwroot¥_vti_log¥*; INTRUSION
...
READ, C:¥Inetpub¥wwwroot¥*; RECON
...
```

FIG. 13

UPDATE OF ACCESS CONTROL LIST

ADDITION

SOURCE IP ADDRESS (SRC)	DESTINATION IP ADDRESS (DST)	PACKET FILTERING PROCESS (PROC)
12.34.56.78	*	DROP
*	1.2.3.1	ACCEPT
*	1.2.3.2	ACCEPT
12.34.1.1	*	ACCEPT
*	1.2.3.3	DROP
*	*	DENY

FIG. 14

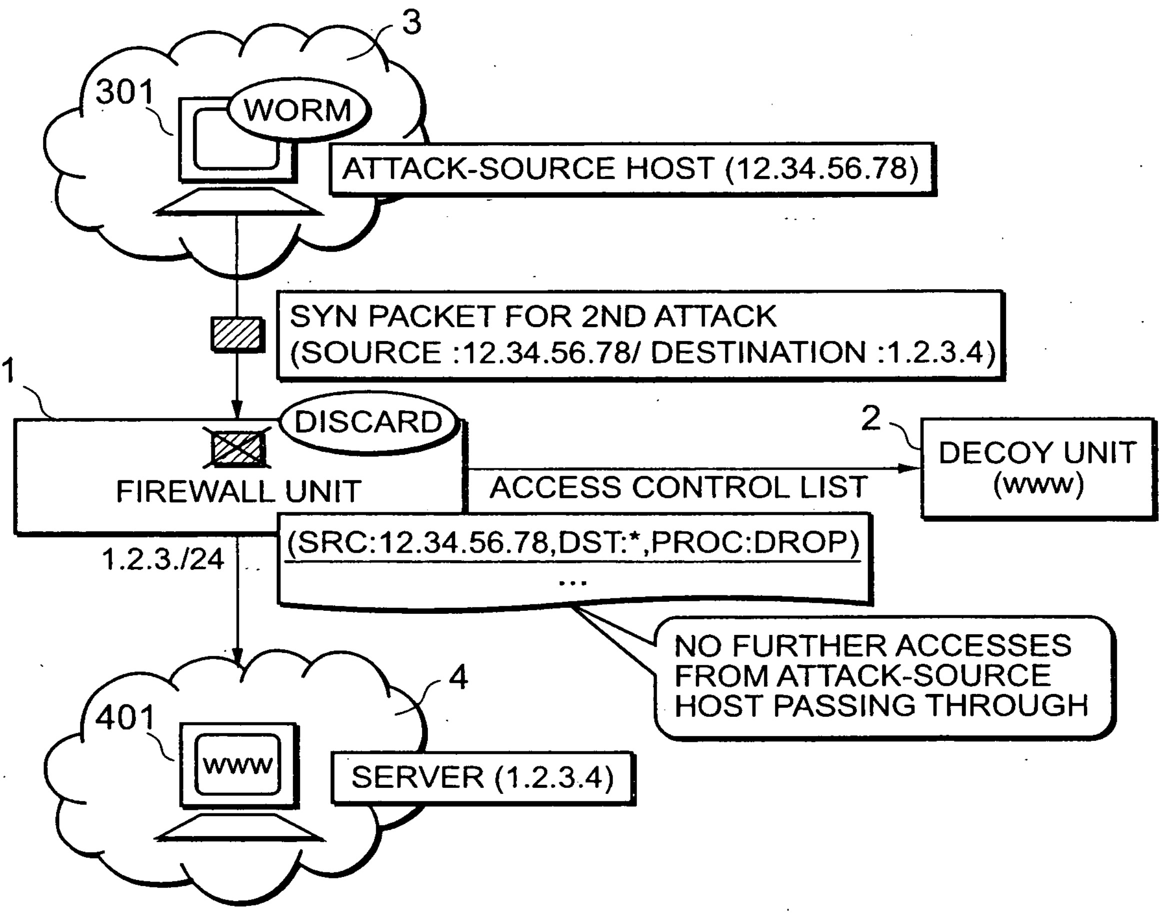
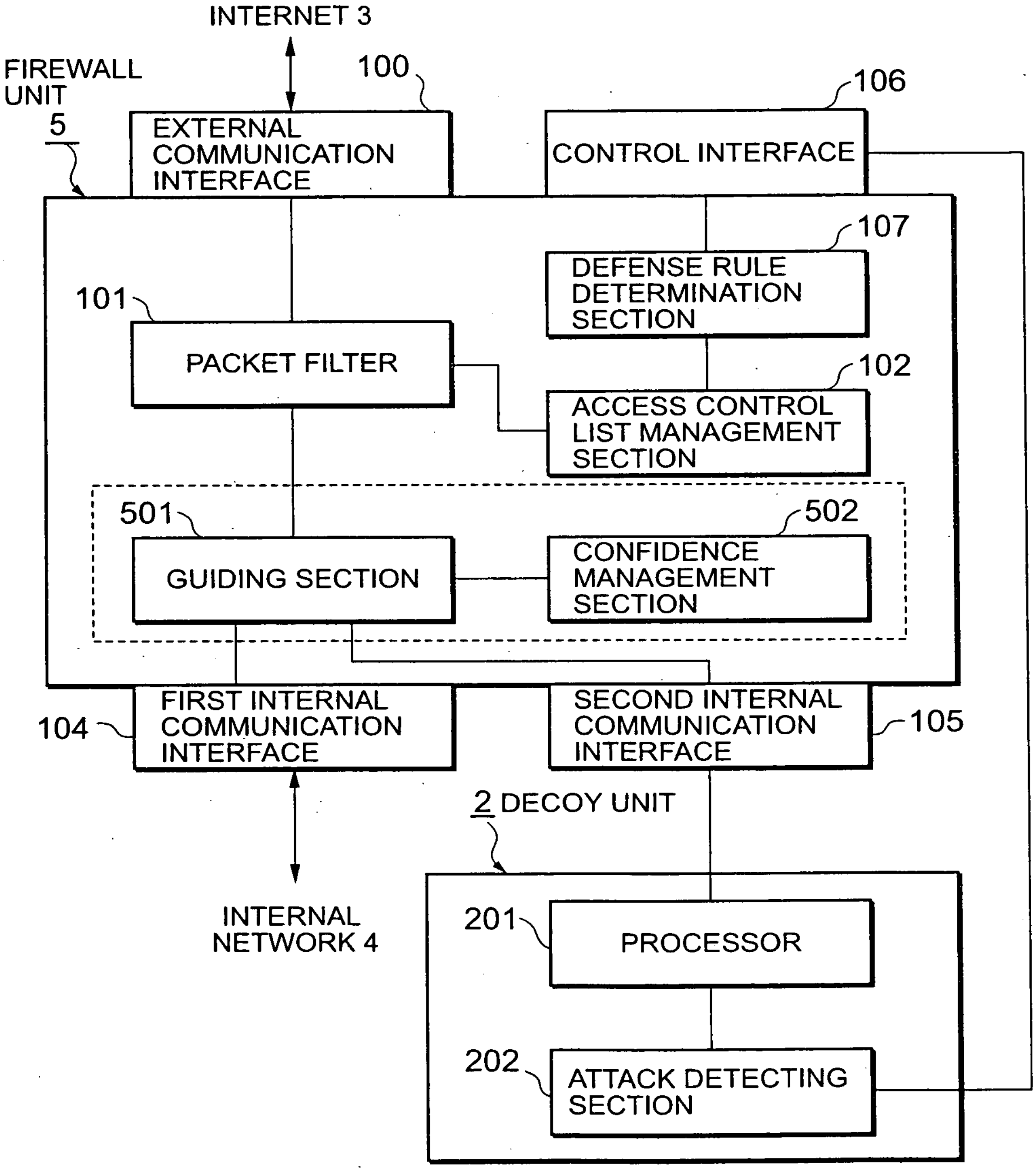

3
301
WORM
ATTACK-SOURCE HOST (12.34.56.78)
SYN PACKET FOR 2ND ATTACK
(SOURCE :12.34.56.78/ DESTINATION :1.2.3.4)
1
DISCARD
FIREWALL UNIT
ACCESS CONTROL LIST
2
DECOY UNIT
(www)
(SRC:12.34.56.78,DST:*,PROC:DROP)
...
1.2.3./24
NO FURTHER ACCESSES FROM ATTACK-SOURCE HOST PASSING THROUGH
4
401
www
SERVER (1.2.3.4)

FIG. 15


INTERNET 3
FIREWALL UNIT
5
100
EXTERNAL COMMUNICATION INTERFACE
106
CONTROL INTERFACE
107
DEFENSE RULE DETERMINATION SECTION
101
PACKET FILTER
102
ACCESS CONTROL LIST MANAGEMENT SECTION
501
GUIDING SECTION
502
CONFIDENCE MANAGEMENT SECTION
104
FIRST INTERNAL COMMUNICATION INTERFACE
SECOND INTERNAL COMMUNICATION INTERFACE
105
2 DECOY UNIT
INTERNAL NETWORK 4
201
PROCESSOR
202
ATTACK DETECTING SECTION

FQ5-613

FIG. 16

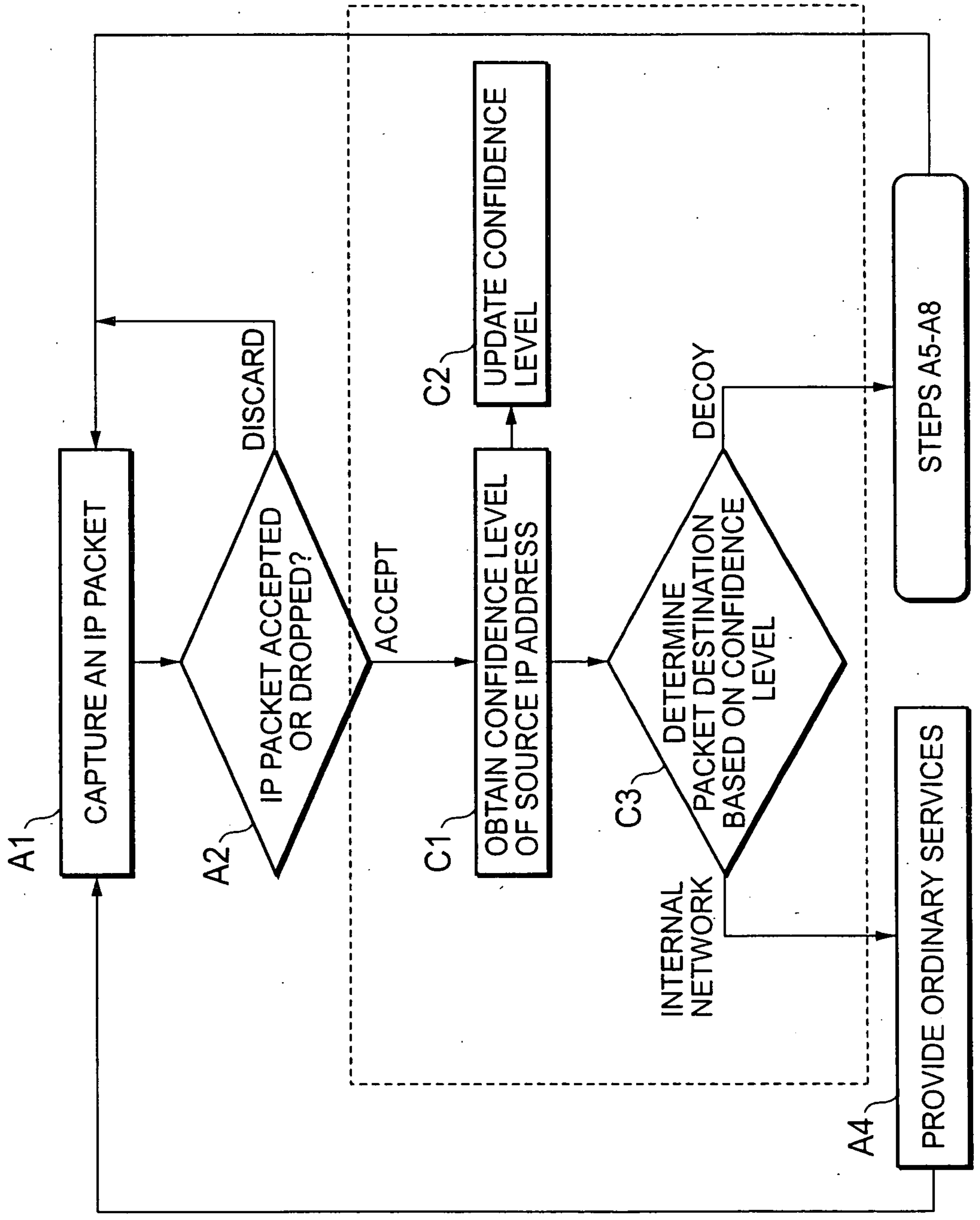

A1
CAPTURE AN IP PACKET
A2
IP PACKET ACCEPTED OR DROPPED?
DISCARD
ACCEPT
C1
OBTAIN CONFIDENCE LEVEL OF SOURCE IP ADDRESS
C2
UPDATE CONFIDENCE LEVEL
C3
DETERMINE PACKET DESTINATION BASED ON CONFIDENCE LEVEL
DECOY
INTERNAL NETWORK
STEPS A5-A8
A4
PROVIDE ORDINARY SERVICES

FIG. 17

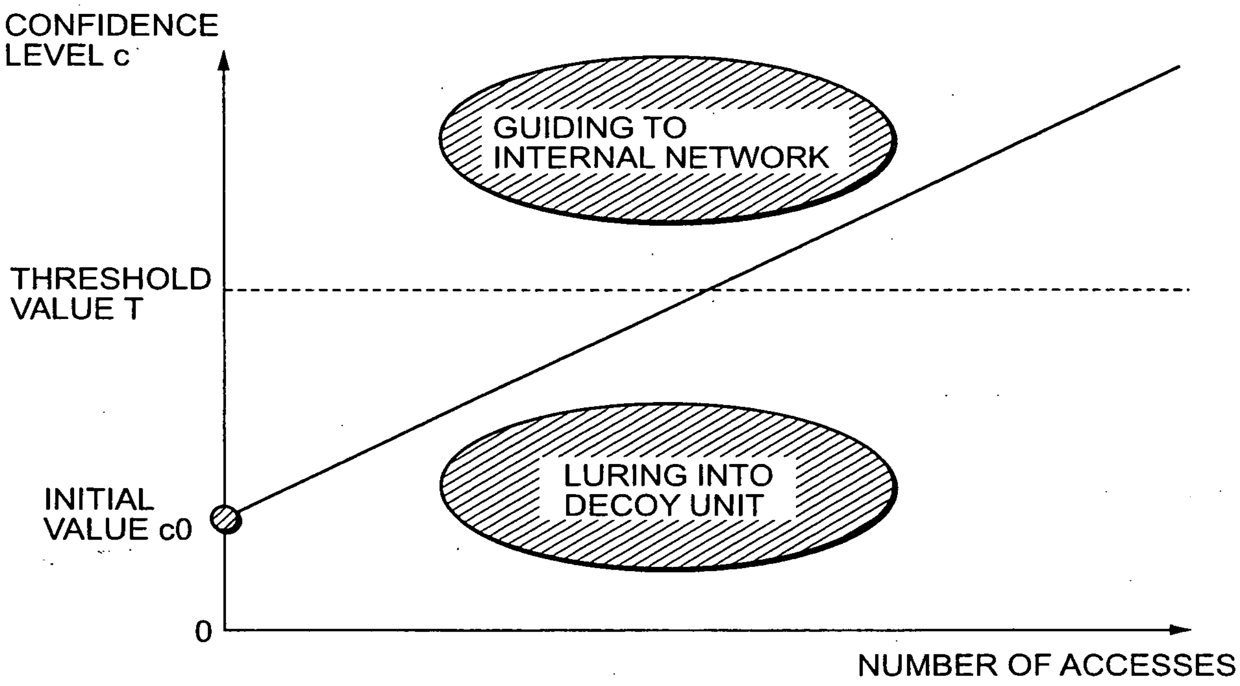

CONFIDENCE LEVEL c
GUIDING TO INTERNAL NETWORK
THRESHOLD VALUE T
LURING INTO DECOY UNIT
INITIAL VALUE c0
0
NUMBER OF ACCESSES

FIG. 18A

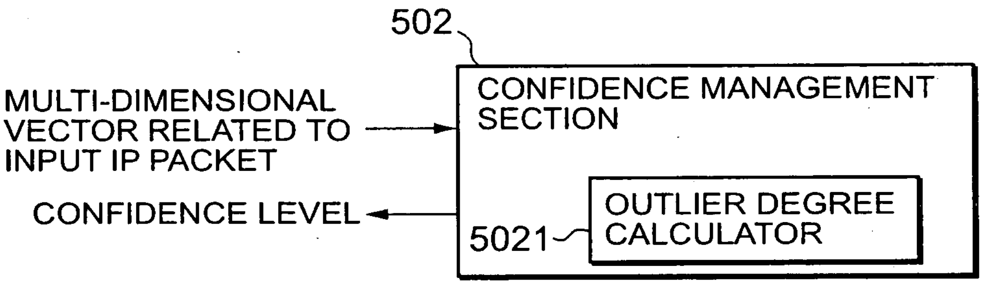

502
CONFIDENCE MANAGEMENT SECTION
MULTI-DIMENSIONAL VECTOR RELATED TO INPUT IP PACKET
CONFIDENCE LEVEL
5021
OUTLIER DEGREE CALCULATOR

FIG. 18B

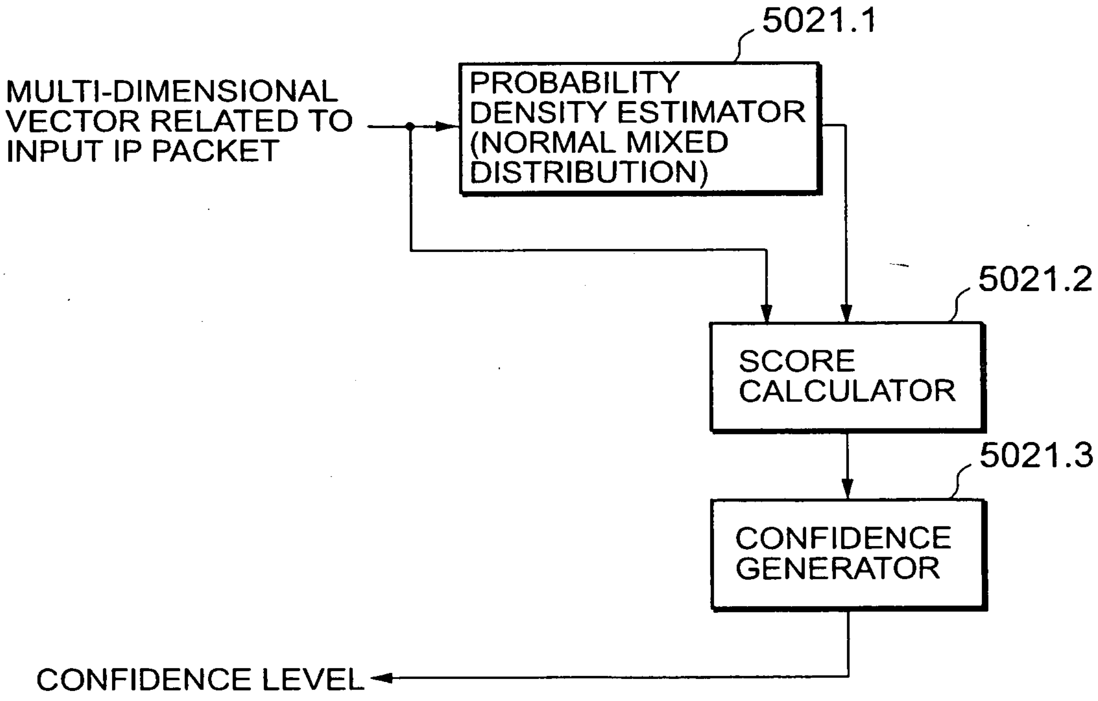

5021.1
MULTI-DIMENSIONAL VECTOR RELATED TO INPUT IP PACKET
PROBABILITY DENSITY ESTIMATOR (NORMAL MIXED DISTRIBUTION)
5021.2
SCORE CALCULATOR
5021.3
CONFIDENCE GENERATOR
CONFIDENCE LEVEL

FIG. 19

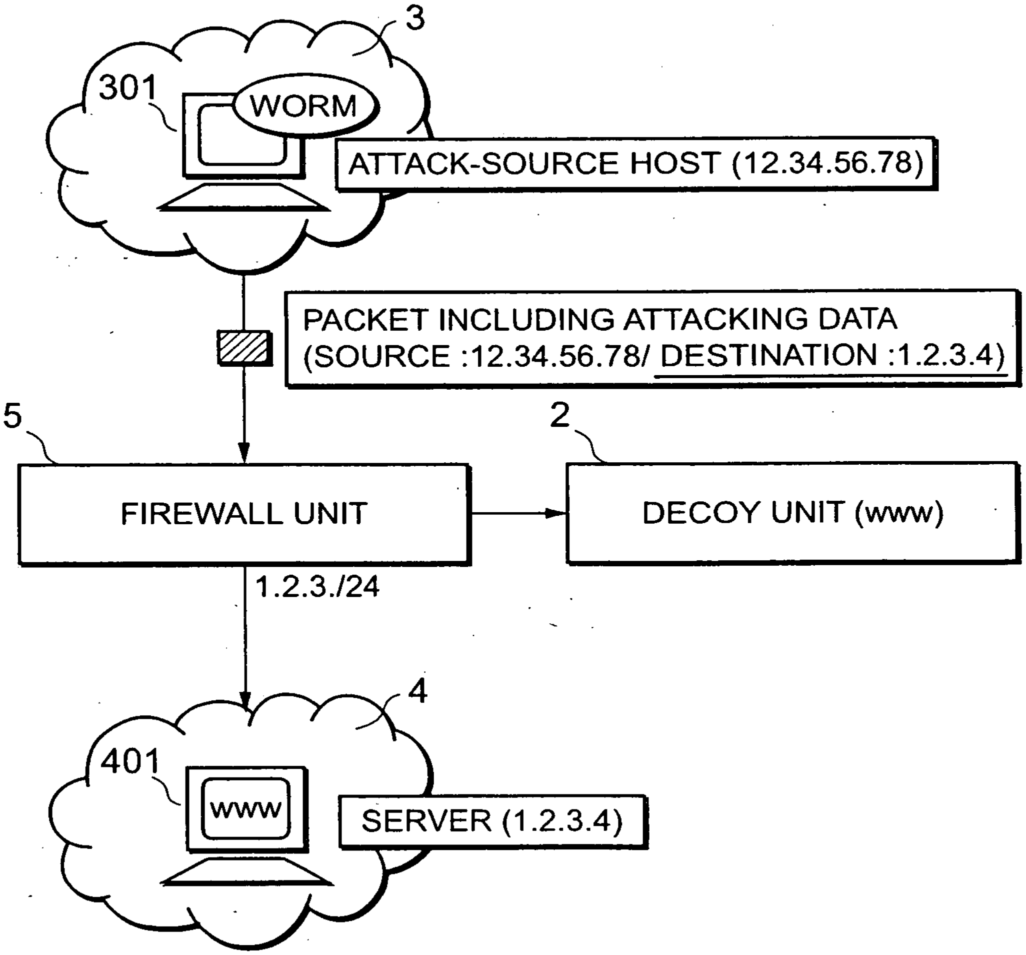

3
301
WORM
ATTACK-SOURCE HOST (12.34.56.78)
PACKET INCLUDING ATTACKING DATA
(SOURCE :12.34.56.78/ DESTINATION :1.2.3.4)
5
2
FIREWALL UNIT
DECOY UNIT (www)
1.2.3./24
4
401
www
SERVER (1.2.3.4)

FIG. 20

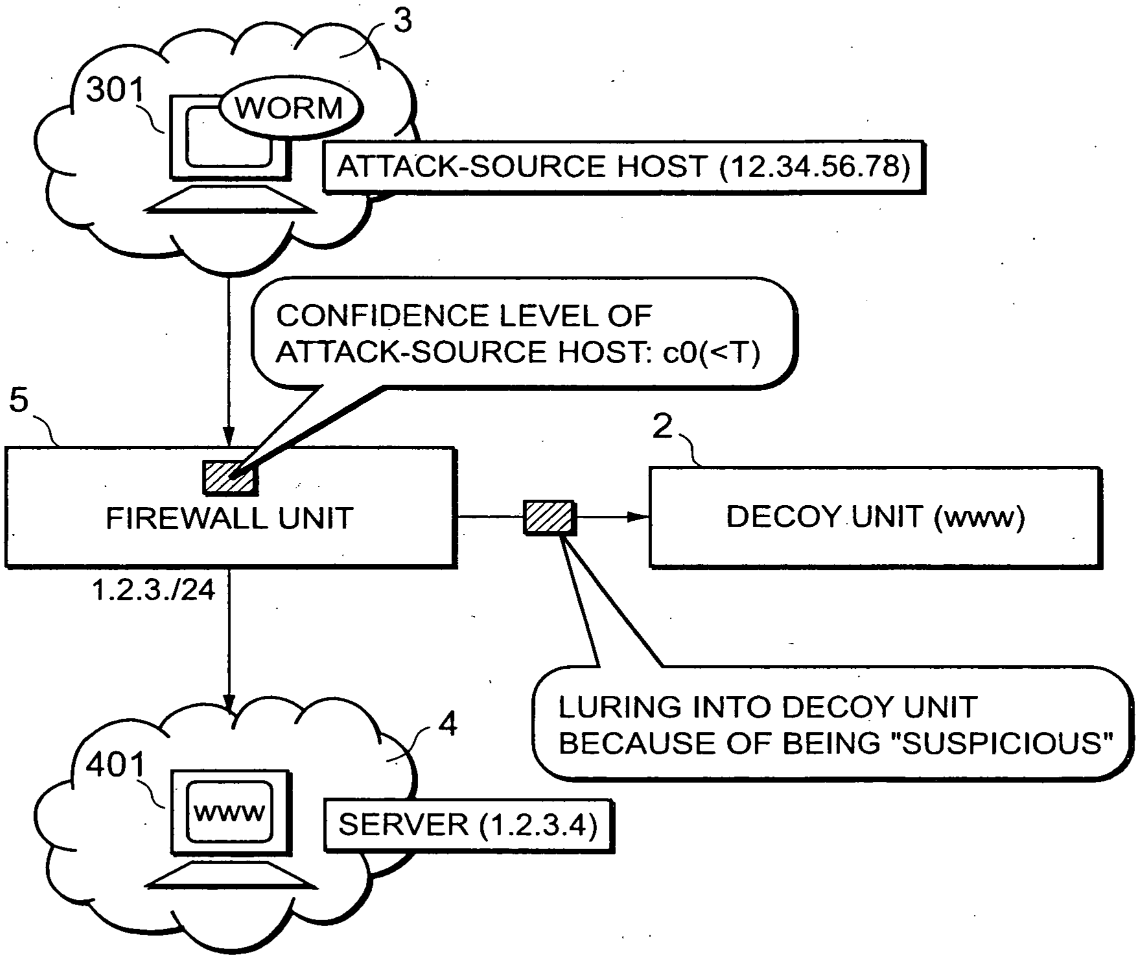

3
301
WORM
ATTACK-SOURCE HOST (12.34.56.78)
CONFIDENCE LEVEL OF
ATTACK-SOURCE HOST: c0(<T)
5
FIREWALL UNIT
2
DECOY UNIT (www)
1.2.3./24
LURING INTO DECOY UNIT
BECAUSE OF BEING "SUSPICIOUS"
4
401
www
SERVER (1.2.3.4)

FIG. 21

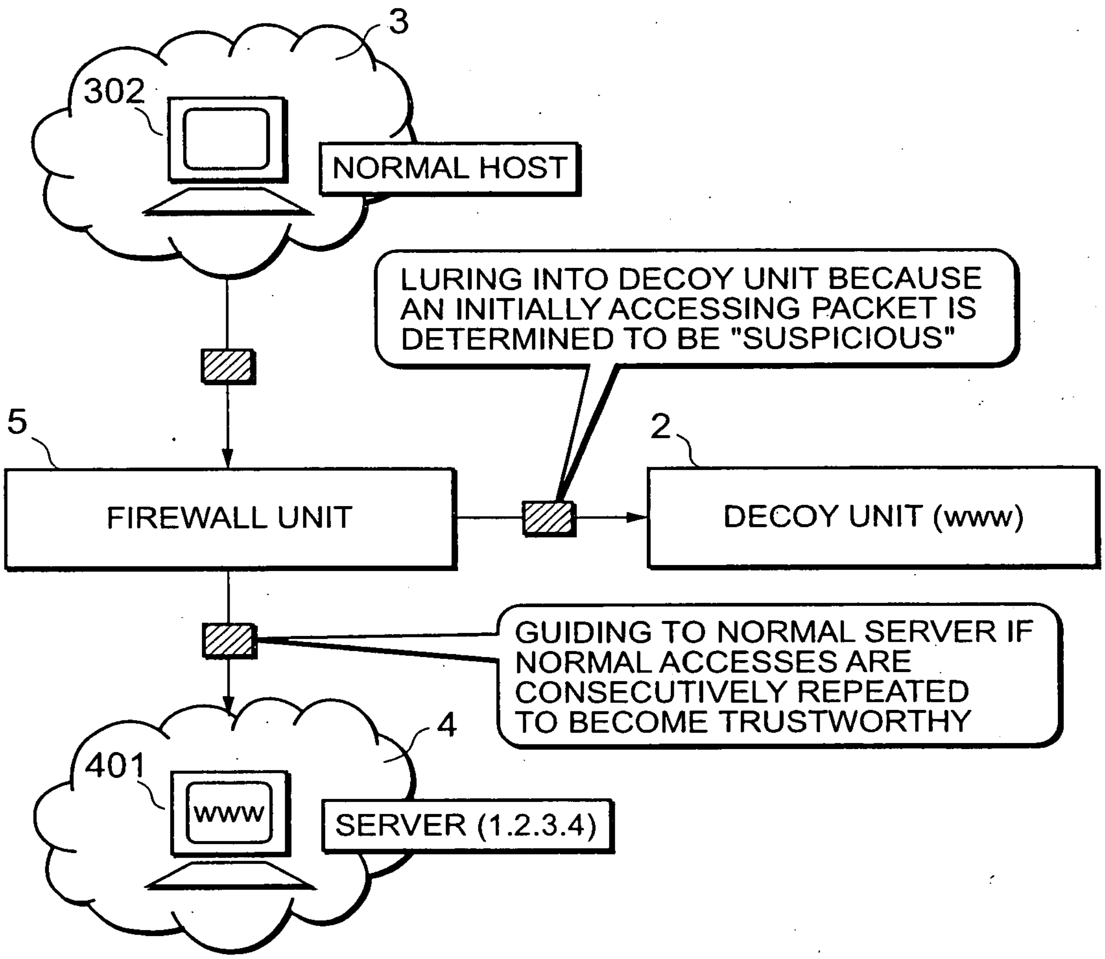

3
302
NORMAL HOST
LURING INTO DECOY UNIT BECAUSE AN INITIALLY ACCESSING PACKET IS DETERMINED TO BE "SUSPICIOUS"
5
2
FIREWALL UNIT
DECOY UNIT (www)
GUIDING TO NORMAL SERVER IF NORMAL ACCESSES ARE CONSECUTIVELY REPEATED TO BECOME TRUSTWORTHY
4
401
www
SERVER (1.2.3.4)

FIG. 22

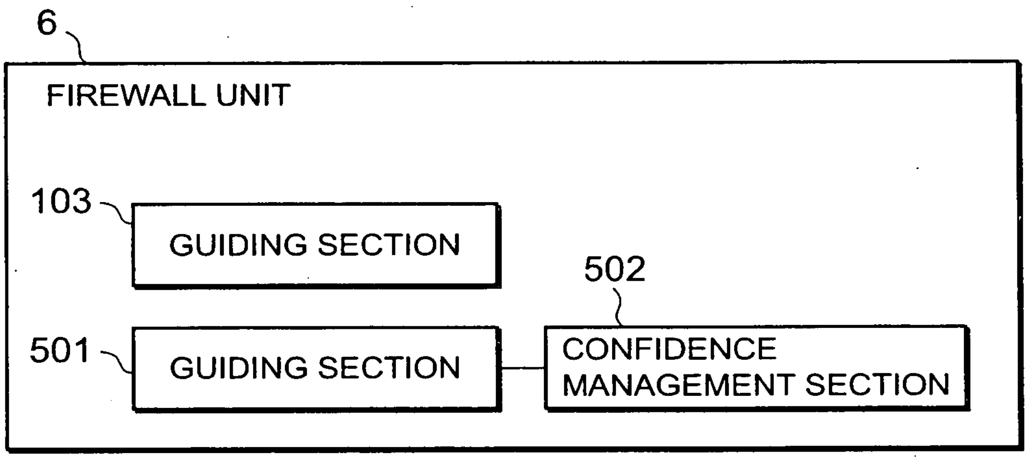

6
FIREWALL UNIT
103
GUIDING SECTION
502
501
GUIDING SECTION
CONFIDENCE
MANAGEMENT SECTION

FIG. 23

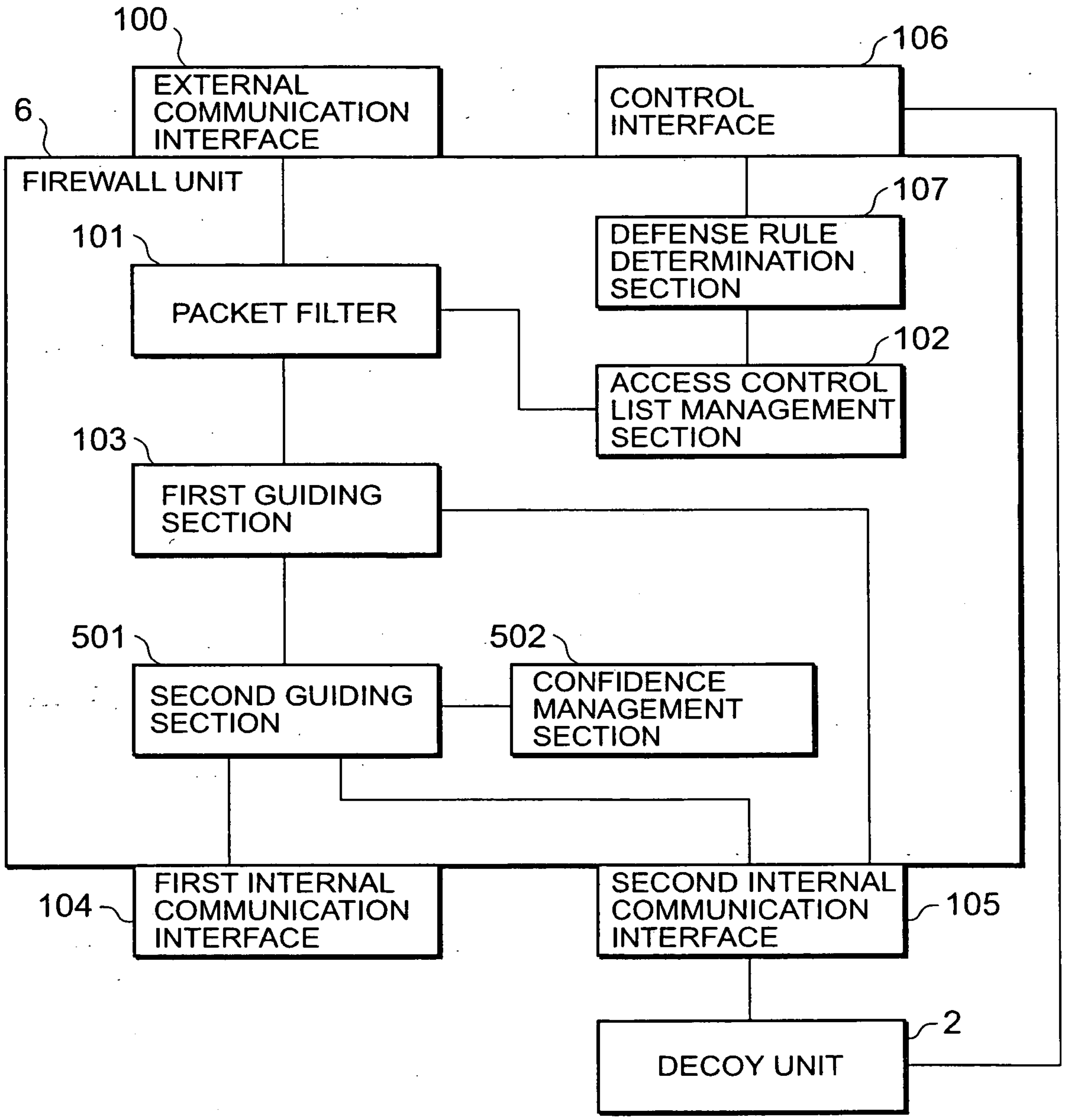

100
EXTERNAL COMMUNICATION INTERFACE
106
CONTROL INTERFACE
6
FIREWALL UNIT
101
PACKET FILTER
107
DEFENSE RULE DETERMINATION SECTION
102
ACCESS CONTROL LIST MANAGEMENT SECTION
103
FIRST GUIDING SECTION
501
SECOND GUIDING SECTION
502
CONFIDENCE MANAGEMENT SECTION
104
FIRST INTERNAL COMMUNICATION INTERFACE
SECOND INTERNAL COMMUNICATION INTERFACE
105
2
DECOY UNIT

FIG. 24

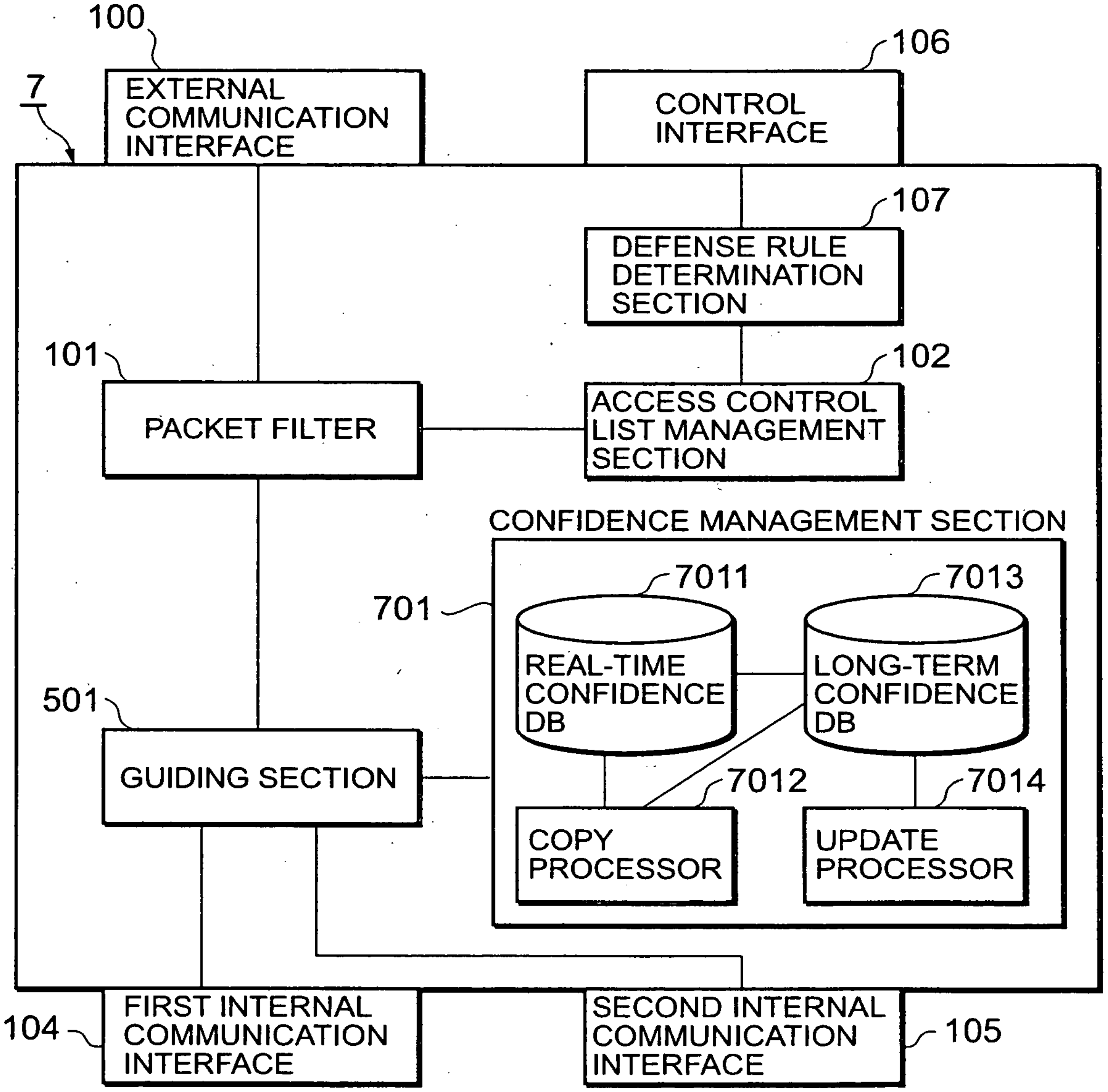

100
EXTERNAL COMMUNICATION INTERFACE
106
CONTROL INTERFACE
7
107
DEFENSE RULE DETERMINATION SECTION
101
PACKET FILTER
102
ACCESS CONTROL LIST MANAGEMENT SECTION
CONFIDENCE MANAGEMENT SECTION
701
7011
REAL-TIME CONFIDENCE DB
7013
LONG-TERM CONFIDENCE DB
501
GUIDING SECTION
7012
COPY PROCESSOR
7014
UPDATE PROCESSOR
104
FIRST INTERNAL COMMUNICATION INTERFACE
SECOND INTERNAL COMMUNICATION INTERFACE
105

FIG. 25

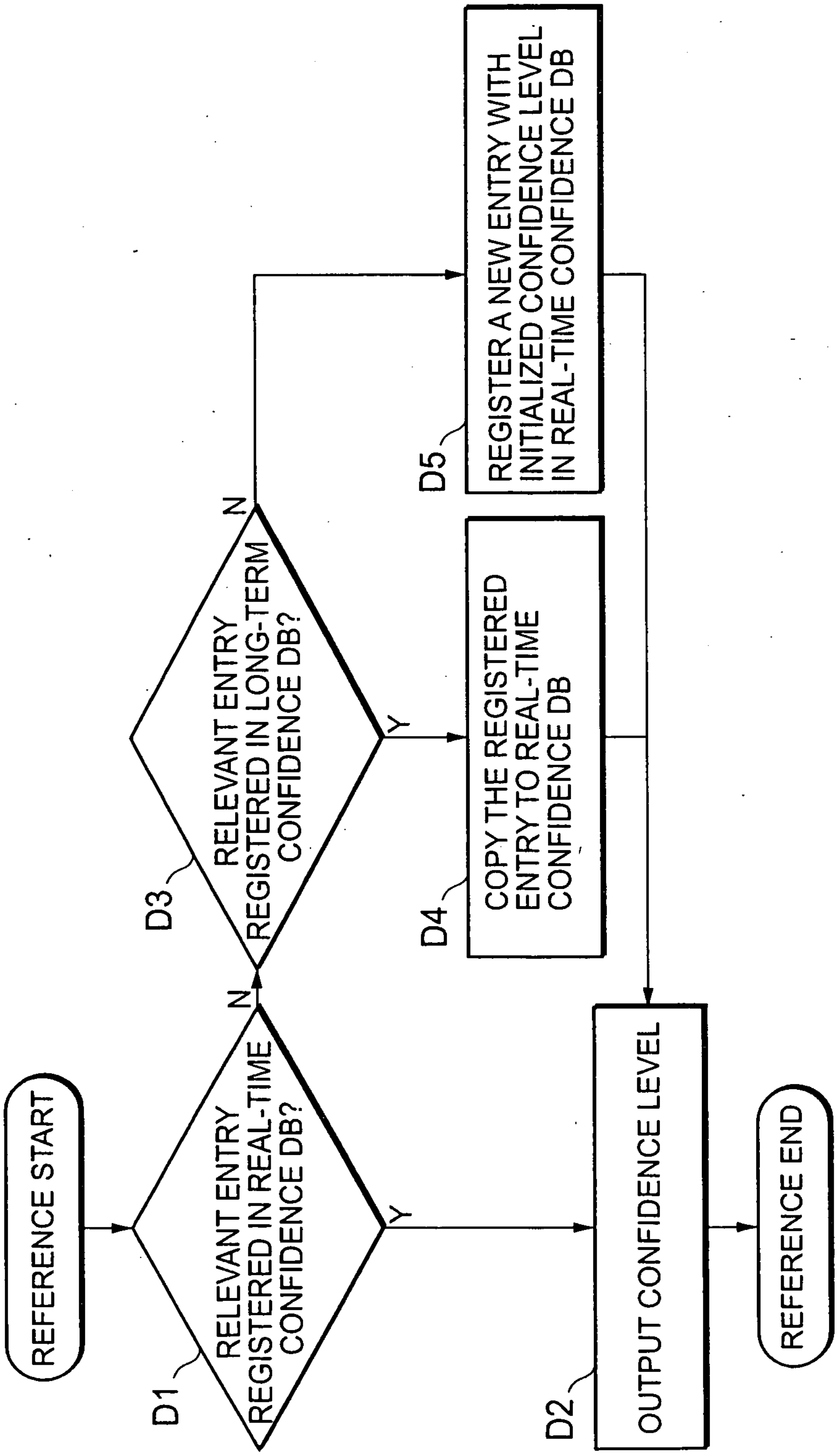

REFERENCE START
D1
RELEVANT ENTRY REGISTERED IN REAL-TIME CONFIDENCE DB?
Y
N
D2
OUTPUT CONFIDENCE LEVEL
REFERENCE END
D3
RELEVANT ENTRY REGISTERED IN LONG-TERM CONFIDENCE DB?
Y
N
D4
COPY THE REGISTERED ENTRY TO REAL-TIME CONFIDENCE DB
D5
REGISTER A NEW ENTRY WITH INITIALIZED CONFIDENCE LEVEL IN REAL-TIME CONFIDENCE DB

FIG. 26

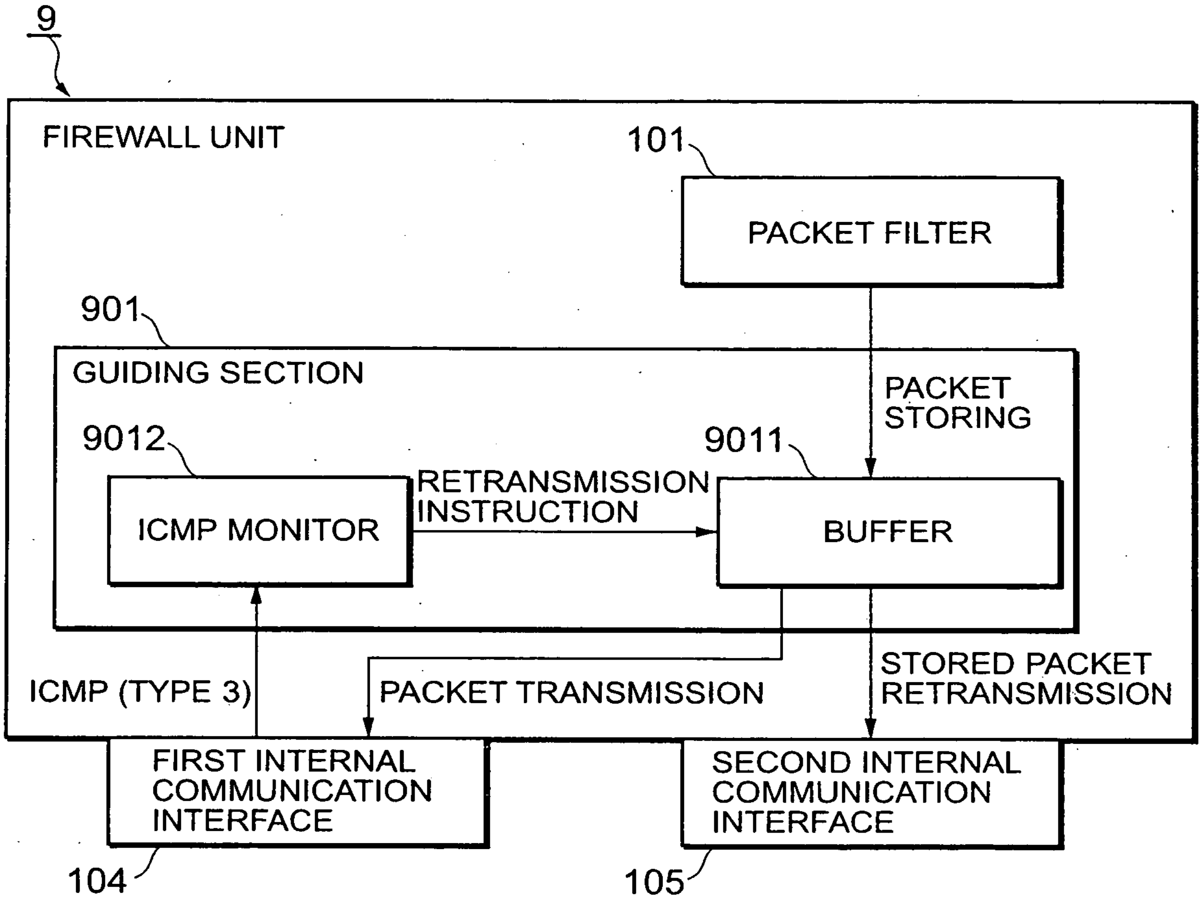

9
FIREWALL UNIT
101
PACKET FILTER
901
GUIDING SECTION
PACKET STORING
9012
9011
ICMP MONITOR
RETRANSMISSION INSTRUCTION
BUFFER
ICMP (TYPE 3)
PACKET TRANSMISSION
STORED PACKET RETRANSMISSION
FIRST INTERNAL COMMUNICATION INTERFACE
SECOND INTERNAL COMMUNICATION INTERFACE
104
105

FIG. 27

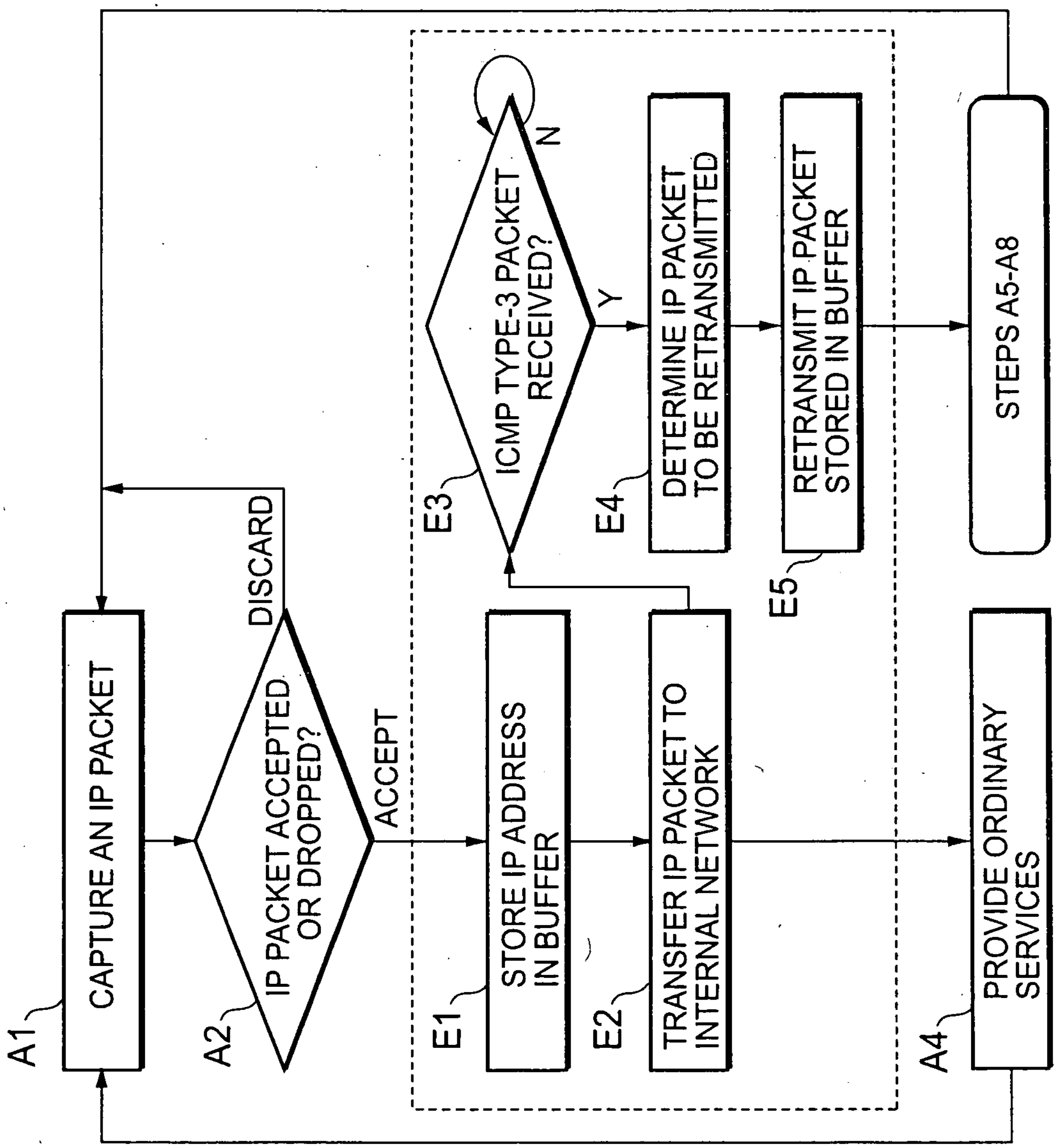
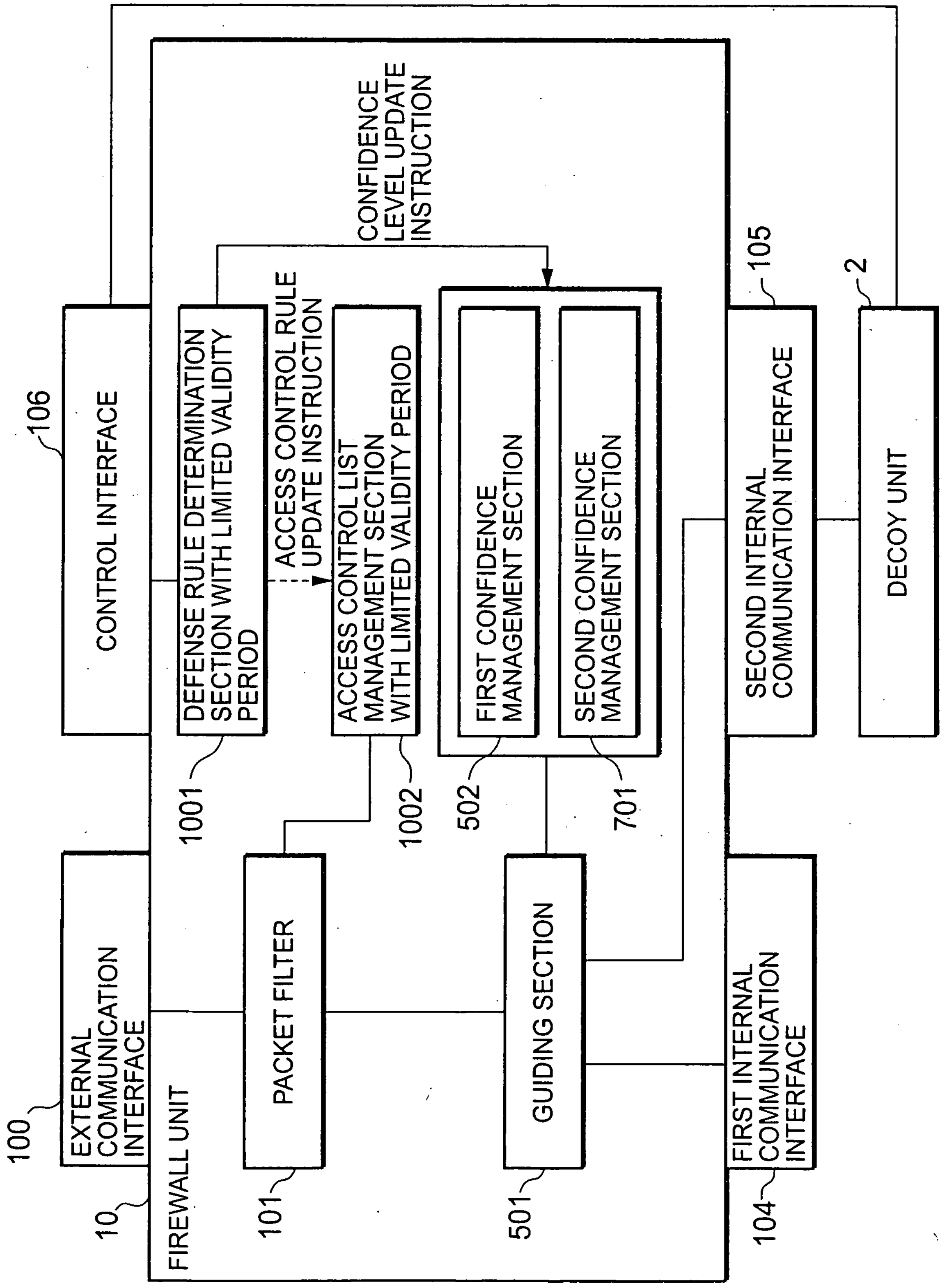

A1
CAPTURE AN IP PACKET
A2
IP PACKET ACCEPTED OR DROPPED?
DISCARD
ACCEPT
E1
STORE IP ADDRESS IN BUFFER
E2
TRANSFER IP PACKET TO INTERNAL NETWORK
E3
ICMP TYPE-3 PACKET RECEIVED?
N
Y
E4
DETERMINE IP PACKET TO BE RETRANSMITTED
E5
RETRANSMIT IP PACKET STORED IN BUFFER
A4
PROVIDE ORDINARY SERVICES
STEPS A5-A8

FIG. 28



100
EXTERNAL COMMUNICATION INTERFACE
106
CONTROL INTERFACE
10
FIREWALL UNIT
101
PACKET FILTER
1001
DEFENSE RULE DETERMINATION SECTION WITH LIMITED VALIDITY PERIOD
ACCESS CONTROL RULE UPDATE INSTRUCTION
1002
ACCESS CONTROL LIST MANAGEMENT SECTION WITH LIMITED VALIDITY PERIOD
CONFIDENCE LEVEL UPDATE INSTRUCTION
502
FIRST CONFIDENCE MANAGEMENT SECTION
701
SECOND CONFIDENCE MANAGEMENT SECTION
501
GUIDING SECTION
104
FIRST INTERNAL COMMUNICATION INTERFACE
105
SECOND INTERNAL COMMUNICATION INTERFACE
2
DECOY UNIT

FIG. 29

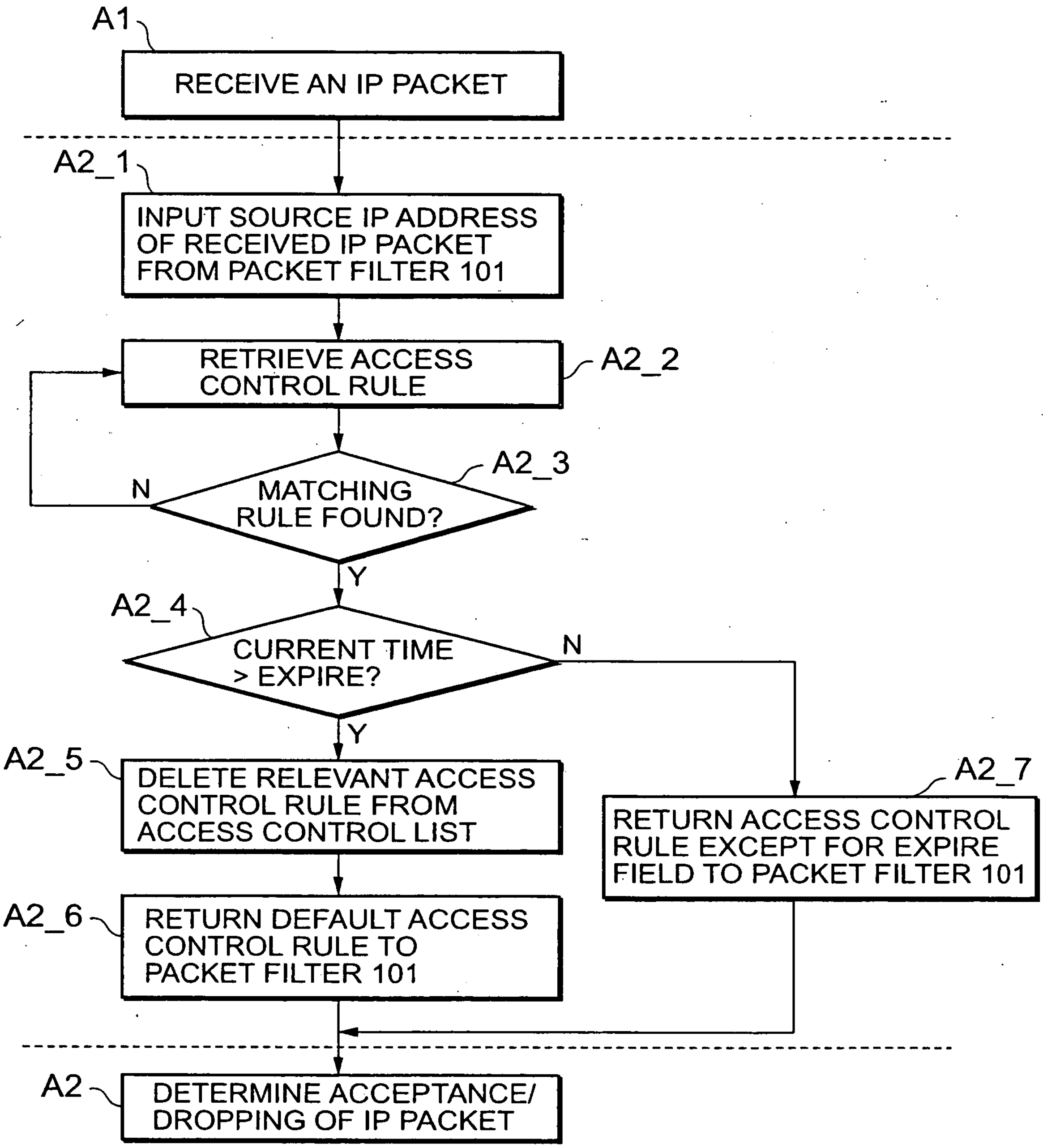

A1
RECEIVE AN IP PACKET
A2_1
INPUT SOURCE IP ADDRESS OF RECEIVED IP PACKET FROM PACKET FILTER 101
RETRIEVE ACCESS CONTROL RULE
A2_2
A2_3
MATCHING RULE FOUND?
N
Y
A2_4
CURRENT TIME > EXPIRE?
N
Y
A2_5
DELETE RELEVANT ACCESS CONTROL RULE FROM ACCESS CONTROL LIST
A2_7
RETURN ACCESS CONTROL RULE EXCEPT FOR EXPIRE FIELD TO PACKET FILTER 101
A2_6
RETURN DEFAULT ACCESS CONTROL RULE TO PACKET FILTER 101
A2
DETERMINE ACCEPTANCE/ DROPPING OF IP PACKET

FIG. 30

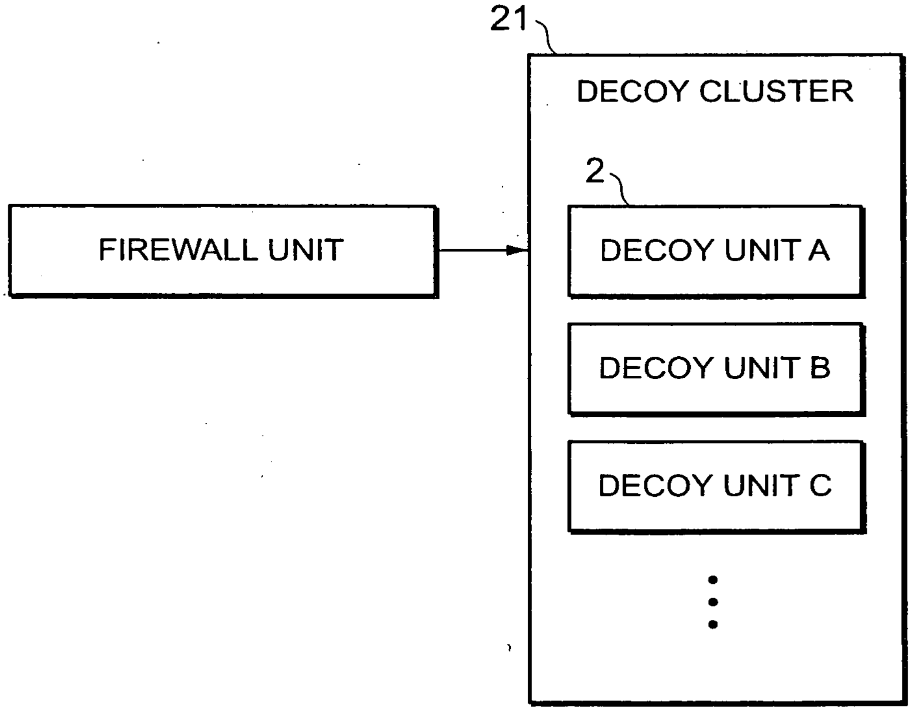

21
DECOY CLUSTER
2
FIREWALL UNIT
DECOY UNIT A
DECOY UNIT B
DECOY UNIT C

FIG. 31

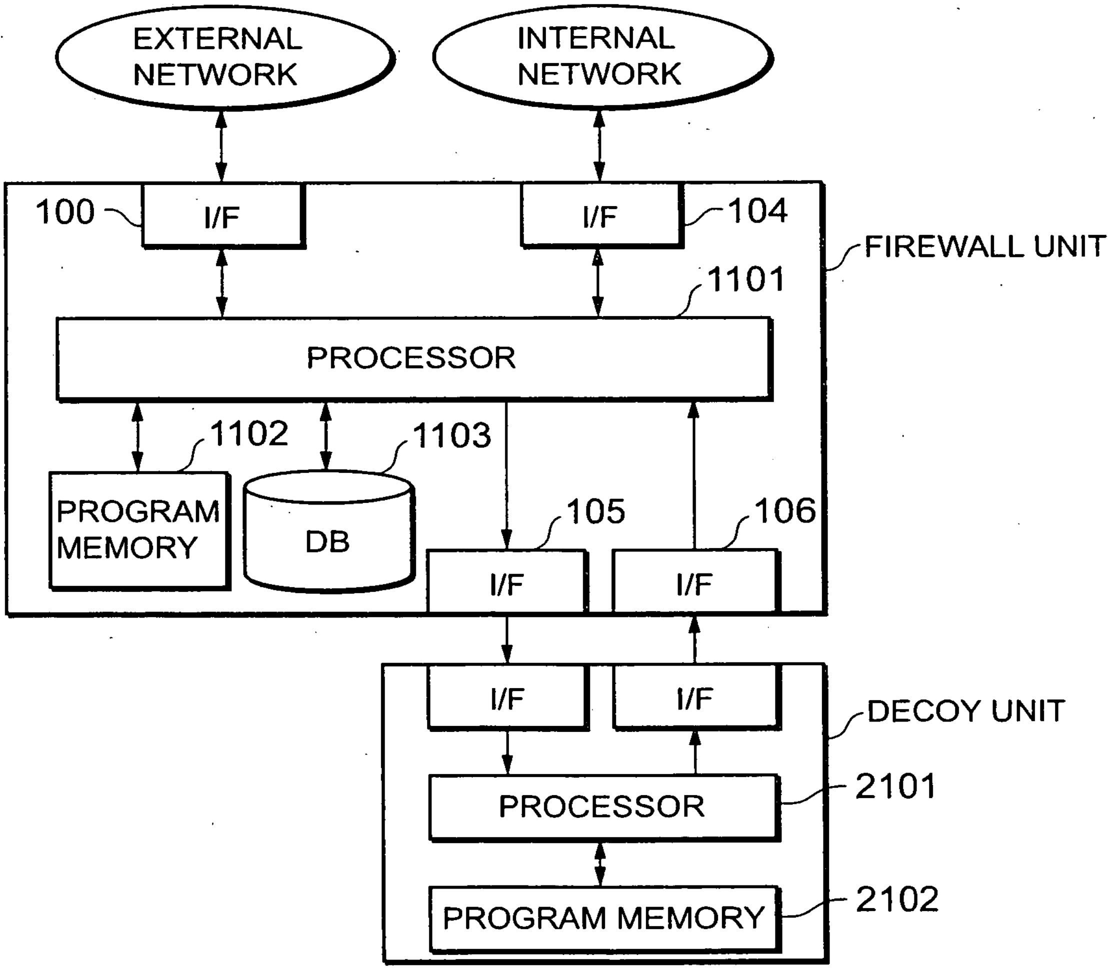

EXTERNAL NETWORK
INTERNAL NETWORK
100
I/F
I/F
104
FIREWALL UNIT
1101
PROCESSOR
1102
1103
PROGRAM MEMORY
DB
105
106
I/F
I/F
I/F
I/F
DECOY UNIT
PROCESSOR
2101
PROGRAM MEMORY
2102

FIG. 32

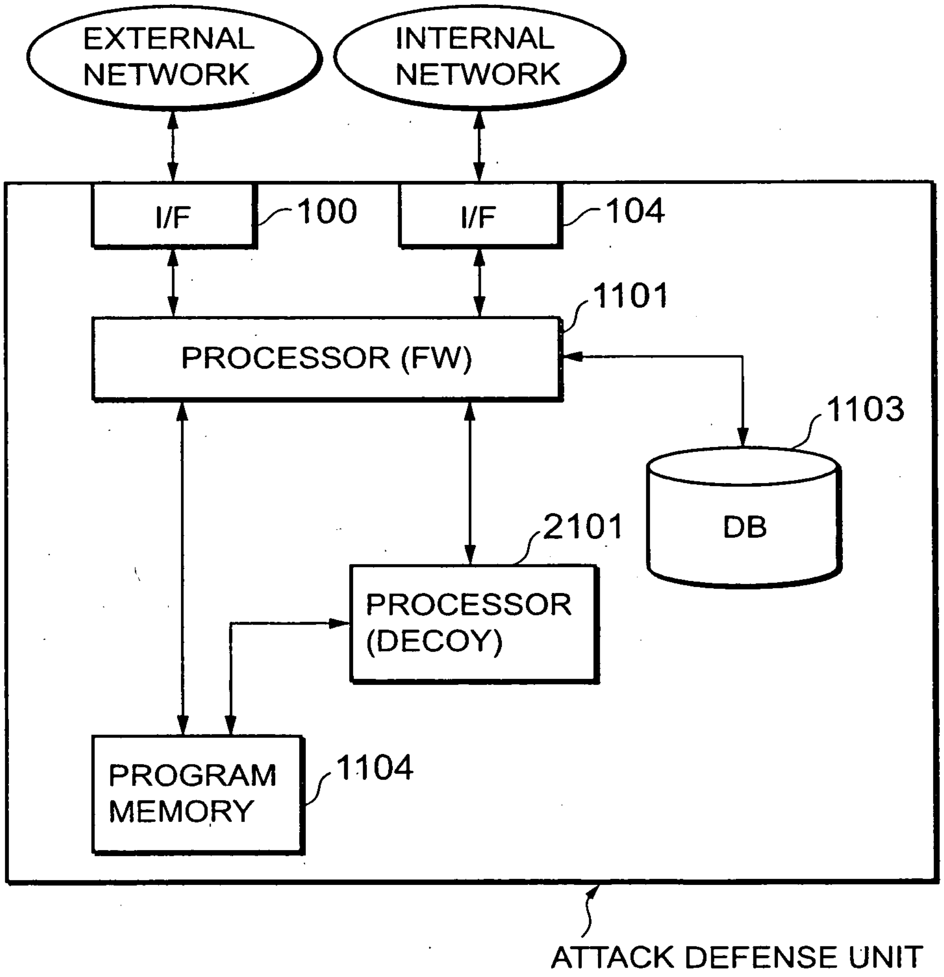

EXTERNAL NETWORK
INTERNAL NETWORK
I/F
100
I/F
104
1101
PROCESSOR (FW)
1103
DB
2101
PROCESSOR (DECOY)
PROGRAM MEMORY
1104
ATTACK DEFENSE UNIT

FIG. 33

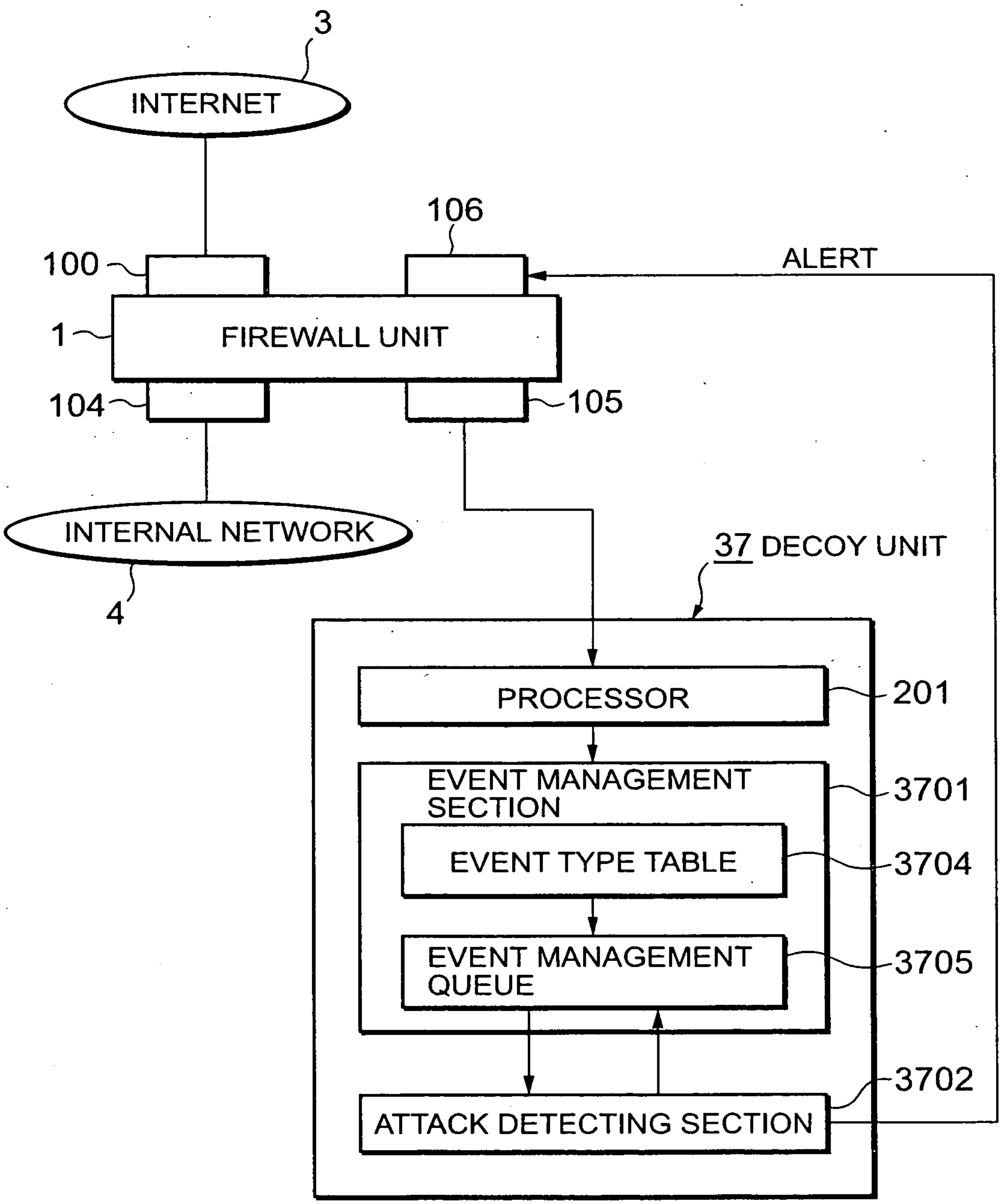

3
INTERNET
106
ALERT
100
1
FIREWALL UNIT
104
105
INTERNAL NETWORK
4
37 DECOY UNIT
PROCESSOR
201
EVENT MANAGEMENT SECTION
3701
EVENT TYPE TABLE
3704
EVENT MANAGEMENT QUEUE
3705
3702
ATTACK DETECTING SECTION

FIG. 34

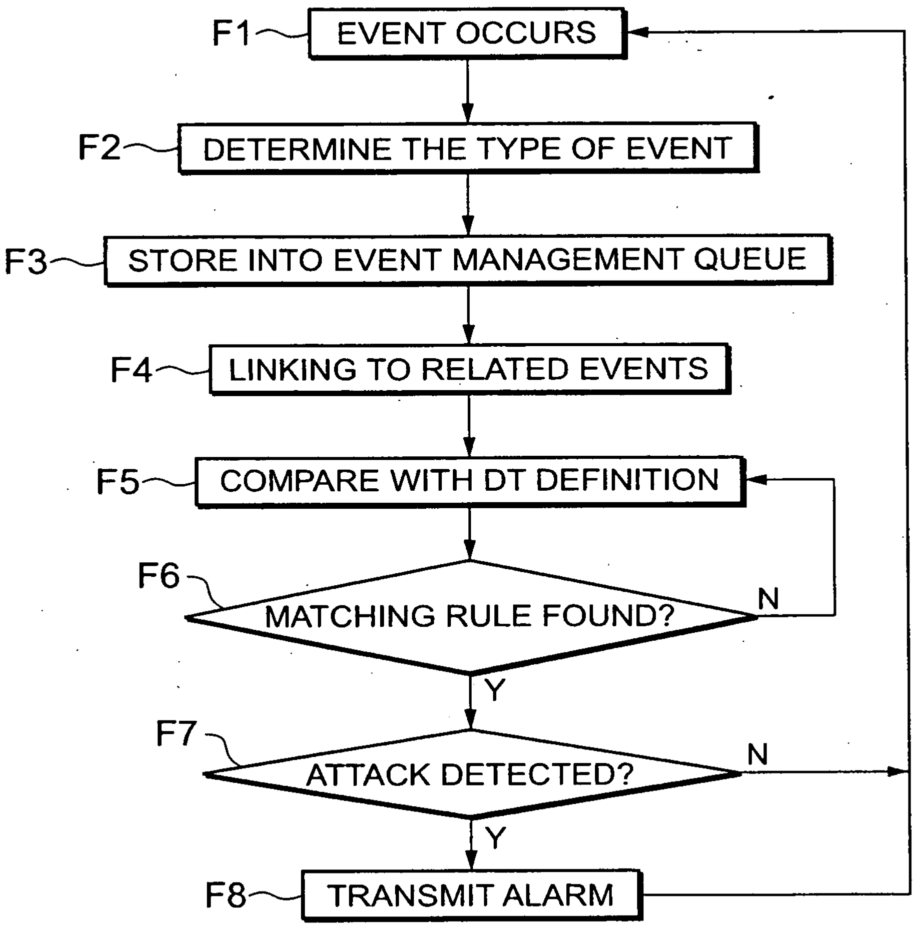
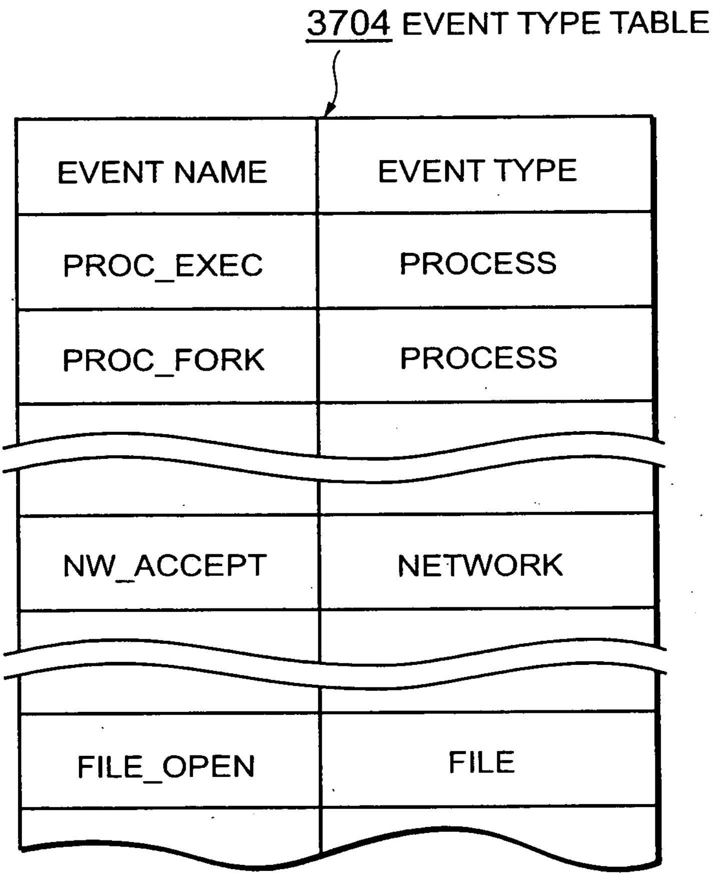

F1
EVENT OCCURS
F2
DETERMINE THE TYPE OF EVENT
F3
STORE INTO EVENT MANAGEMENT QUEUE
F4
LINKING TO RELATED EVENTS
F5
COMPARE WITH DT DEFINITION
F6
MATCHING RULE FOUND?
N
Y
F7
ATTACK DETECTED?
N
Y
F8
TRANSMIT ALARM

FIG. 35


3704 EVENT TYPE TABLE

EVENT NAME	EVENT TYPE
PROC_EXEC	PROCESS
PROC_FORK	PROCESS
NW_ACCEPT	NETWORK
FILE_OPEN	FILE

FIG. 36

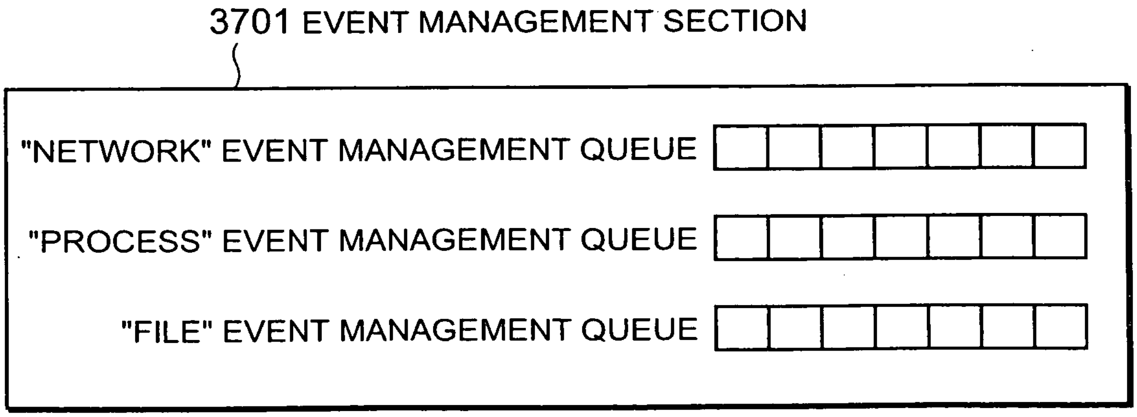

3701 EVENT MANAGEMENT SECTION
"NETWORK" EVENT MANAGEMENT QUEUE
"PROCESS" EVENT MANAGEMENT QUEUE
"FILE" EVENT MANAGEMENT QUEUE

FIG. 37

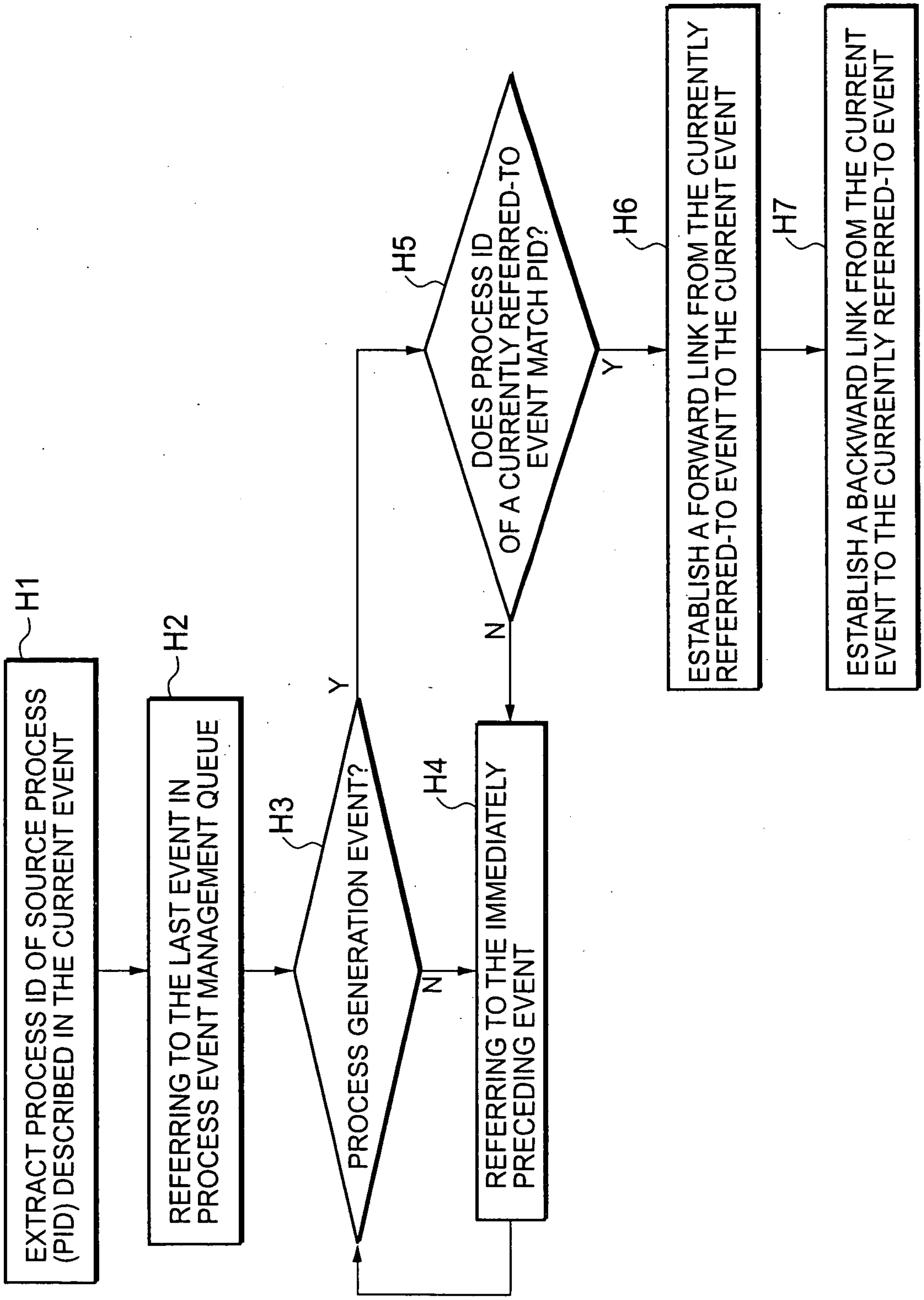

H1
EXTRACT PROCESS ID OF SOURCE PROCESS (PID) DESCRIBED IN THE CURRENT EVENT
H2
REFERRING TO THE LAST EVENT IN PROCESS EVENT MANAGEMENT QUEUE
H3
PROCESS GENERATION EVENT?
Y
N
H4
REFERRING TO THE IMMEDIATELY PRECEDING EVENT
H5
DOES PROCESS ID OF A CURRENTLY REFERRED-TO EVENT MATCH PID?
N
Y
H6
ESTABLISH A FORWARD LINK FROM THE CURRENTLY REFERRED-TO EVENT TO THE CURRENT EVENT
H7
ESTABLISH A BACKWARD LINK FROM THE CURRENT EVENT TO THE CURRENTLY REFERRED-TO EVENT

FIG. 38

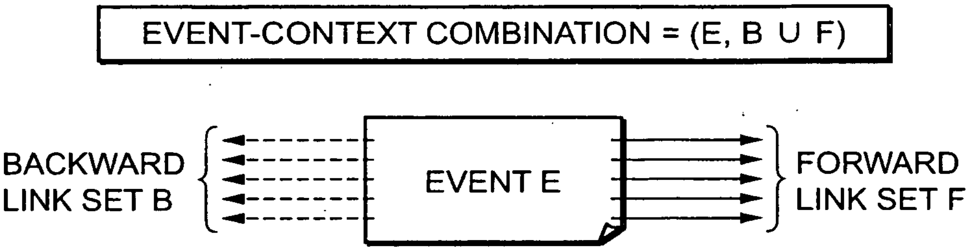
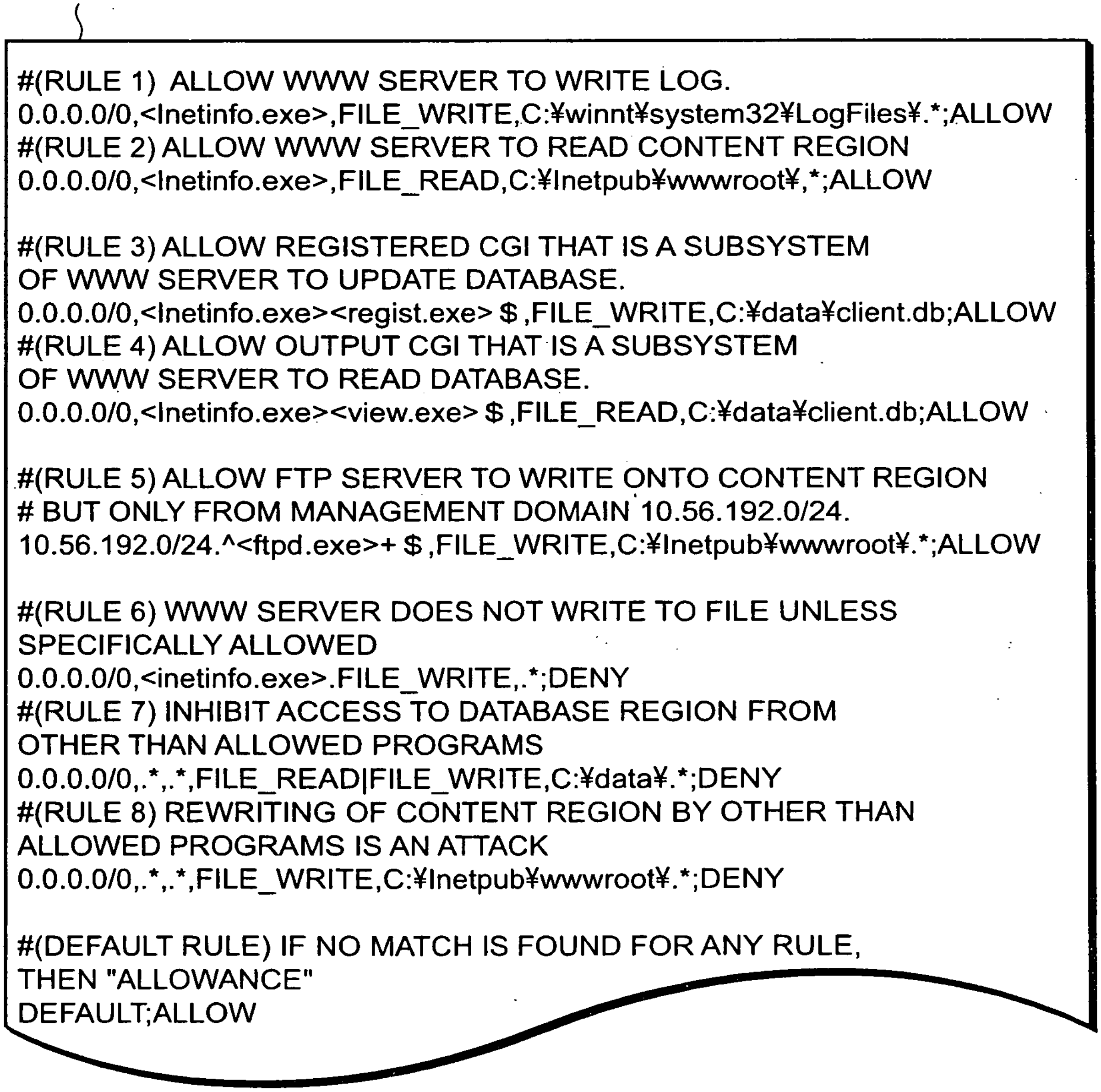


FIG. 39

4101 DT DEFINITION FILE



```
#(RULE 1)  ALLOW WWW SERVER TO WRITE LOG.
0.0.0.0/0,<Inetinfo.exe>,FILE_WRITE,C:¥winnt¥system32¥LogFiles¥.*;ALLOW
#(RULE 2) ALLOW WWW SERVER TO READ CONTENT REGION
0.0.0.0/0,<Inetinfo.exe>,FILE_READ,C:¥Inetpub¥wwwroot¥,*;ALLOW

#(RULE 3) ALLOW REGISTERED CGI THAT IS A SUBSYSTEM
OF WWW SERVER TO UPDATE DATABASE.
0.0.0.0/0,<Inetinfo.exe><regist.exe> $ ,FILE_WRITE,C:¥data¥client.db;ALLOW
#(RULE 4) ALLOW OUTPUT CGI THAT IS A SUBSYSTEM
OF WWW SERVER TO READ DATABASE.
0.0.0.0/0,<Inetinfo.exe><view.exe> $ ,FILE_READ,C:¥data¥client.db;ALLOW

#(RULE 5) ALLOW FTP SERVER TO WRITE ONTO CONTENT REGION
# BUT ONLY FROM MANAGEMENT DOMAIN 10.56.192.0/24.
10.56.192.0/24.^<ftpd.exe>+ $ ,FILE_WRITE,C:¥Inetpub¥wwwroot¥.*;ALLOW

#(RULE 6) WWW SERVER DOES NOT WRITE TO FILE UNLESS
SPECIFICALLY ALLOWED
0.0.0.0/0,<inetinfo.exe>.FILE_WRITE,.*;DENY
#(RULE 7) INHIBIT ACCESS TO DATABASE REGION FROM
OTHER THAN ALLOWED PROGRAMS
0.0.0.0/0,.*,.*,FILE_READ|FILE_WRITE,C:¥data¥.*;DENY
#(RULE 8) REWRITING OF CONTENT REGION BY OTHER THAN
ALLOWED PROGRAMS IS AN ATTACK
0.0.0.0/0,.*,.*,FILE_WRITE,C:¥Inetpub¥wwwroot¥.*;DENY

#(DEFAULT RULE) IF NO MATCH IS FOUND FOR ANY RULE,
THEN "ALLOWANCE"
DEFAULT;ALLOW
```

FIG. 40

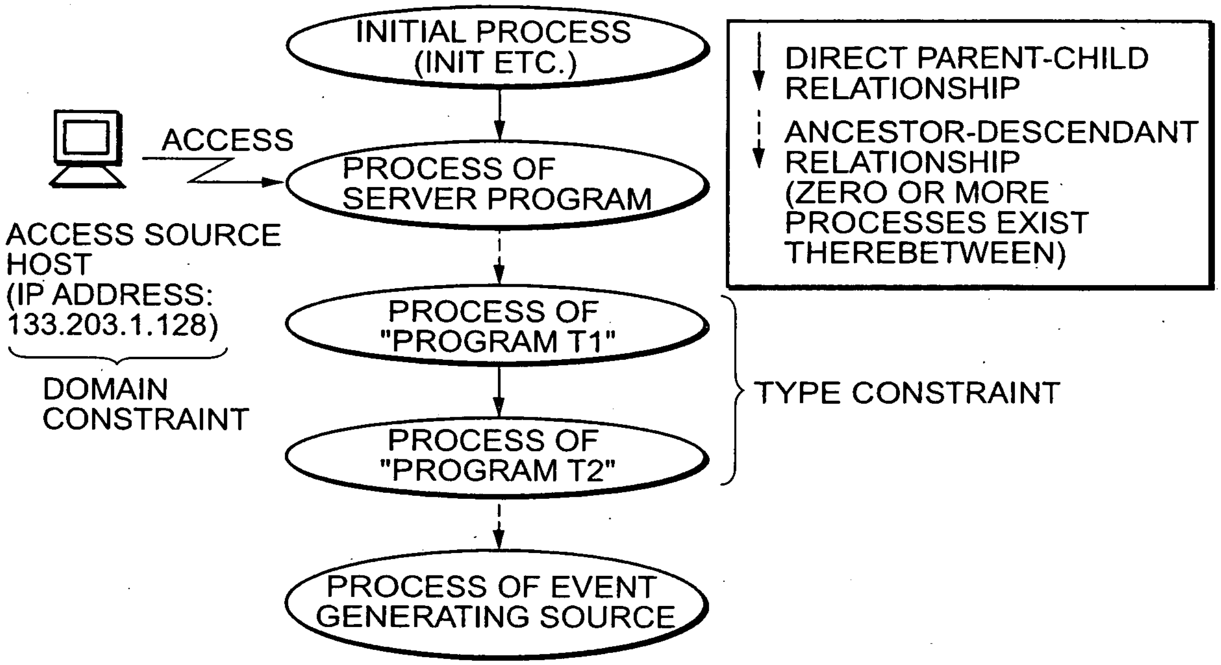
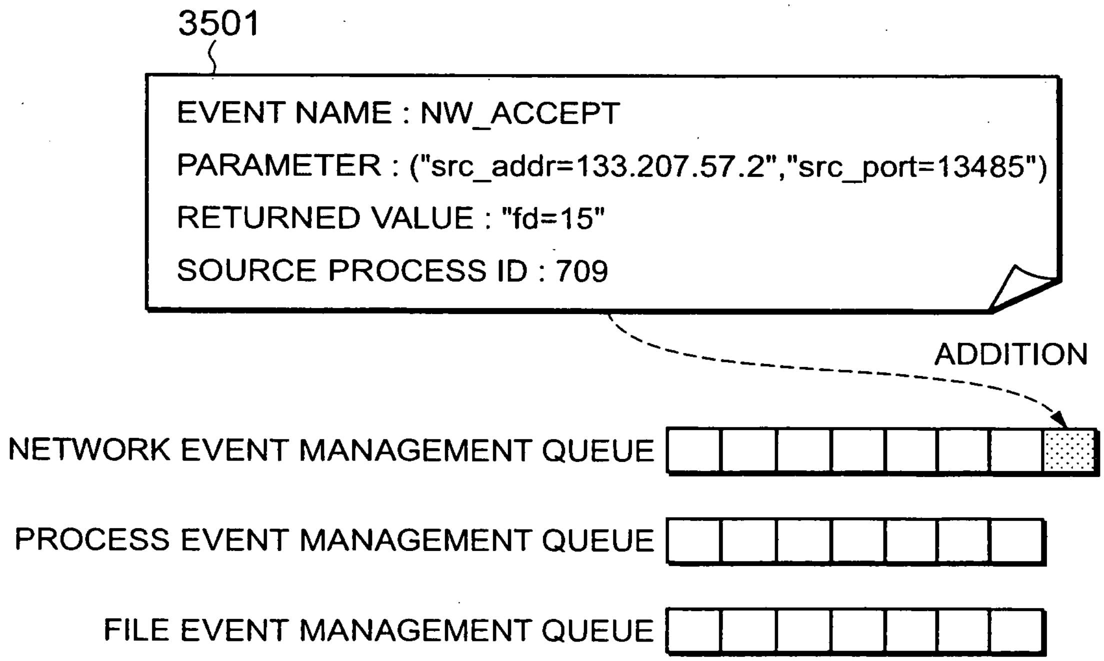

INITIAL PROCESS (INIT ETC.)
ACCESS
PROCESS OF SERVER PROGRAM
ACCESS SOURCE HOST (IP ADDRESS: 133.203.1.128)
DOMAIN CONSTRAINT
PROCESS OF "PROGRAM T1"
PROCESS OF "PROGRAM T2"
TYPE CONSTRAINT
PROCESS OF EVENT GENERATING SOURCE
DIRECT PARENT-CHILD RELATIONSHIP
ANCESTOR-DESCENDANT RELATIONSHIP (ZERO OR MORE PROCESSES EXIST THEREBETWEEN)

FIG. 41


3501
ADDITION
NETWORK EVENT MANAGEMENT QUEUE
PROCESS EVENT MANAGEMENT QUEUE
FILE EVENT MANAGEMENT QUEUE

EVENT NAME : NW_ACCEPT

PARAMETER : ("src_addr=133.207.57.2","src_port=13485")

RETURNED VALUE : "fd=15"

SOURCE PROCESS ID : 709

FIG. 42

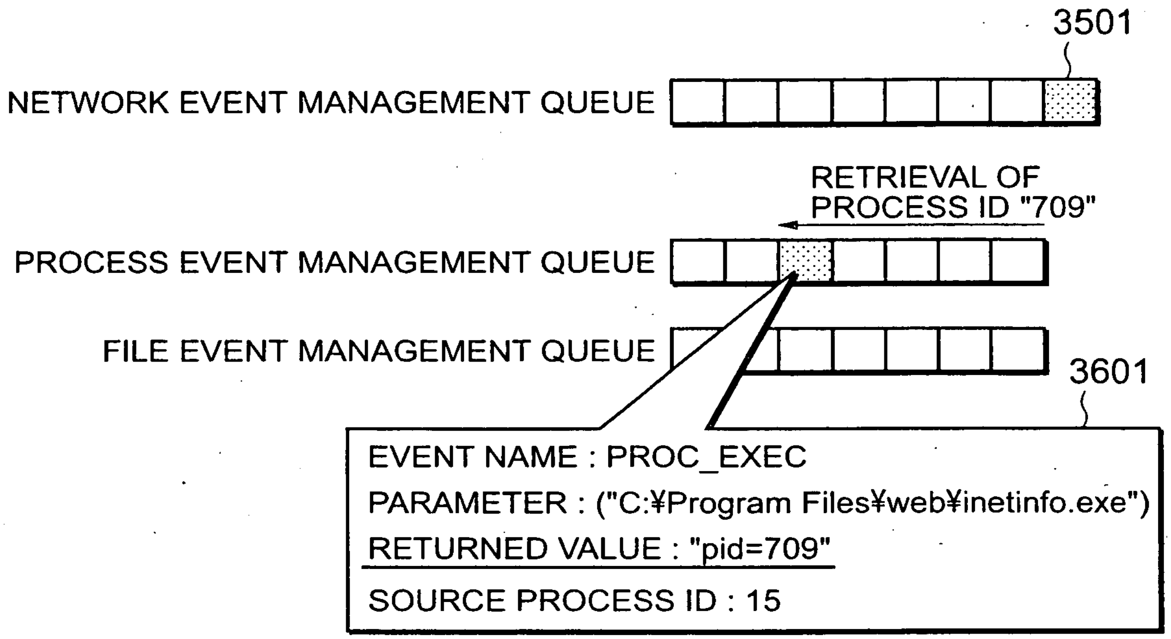

3501
NETWORK EVENT MANAGEMENT QUEUE
RETRIEVAL OF PROCESS ID "709"
PROCESS EVENT MANAGEMENT QUEUE
FILE EVENT MANAGEMENT QUEUE
3601
EVENT NAME : PROC_EXEC
PARAMETER : ("C:¥Program Files¥web¥inetinfo.exe")
RETURNED VALUE : "pid=709"
SOURCE PROCESS ID : 15

FIG. 43

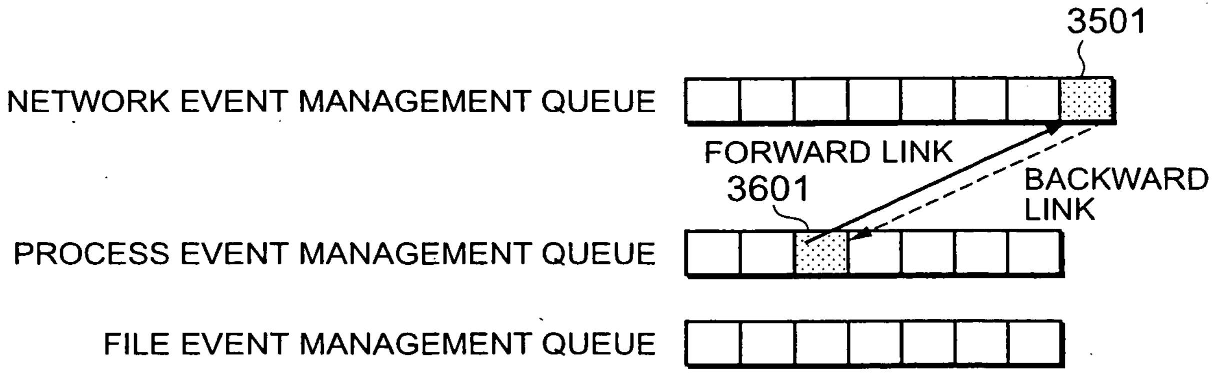

3501
NETWORK EVENT MANAGEMENT QUEUE
FORWARD LINK
3601
BACKWARD LINK
PROCESS EVENT MANAGEMENT QUEUE
FILE EVENT MANAGEMENT QUEUE

FIG. 44

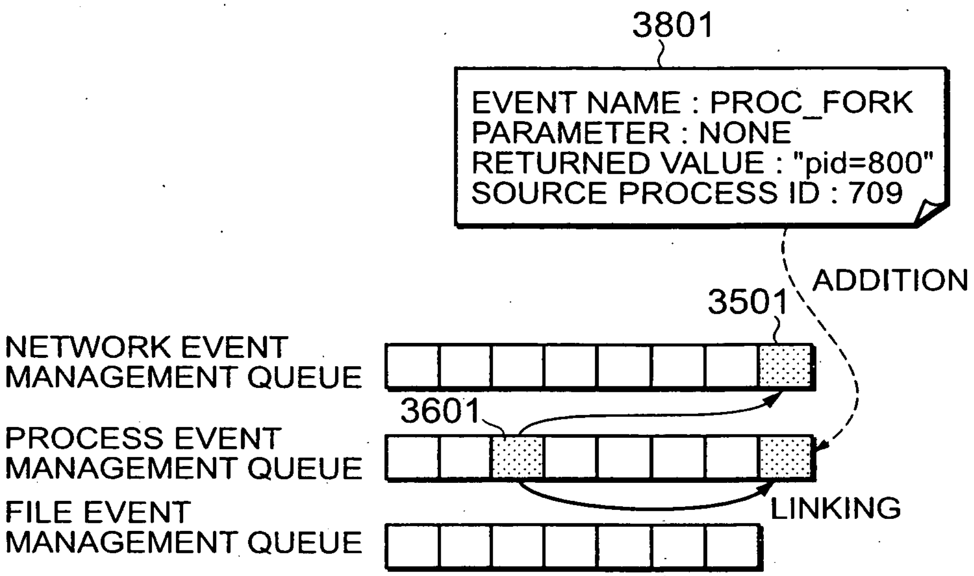

3801
EVENT NAME : PROC_FORK
PARAMETER : NONE
RETURNED VALUE : "pid=800"
SOURCE PROCESS ID : 709
ADDITION
3501
NETWORK EVENT MANAGEMENT QUEUE
3601
PROCESS EVENT MANAGEMENT QUEUE
LINKING
FILE EVENT MANAGEMENT QUEUE

FIG. 45

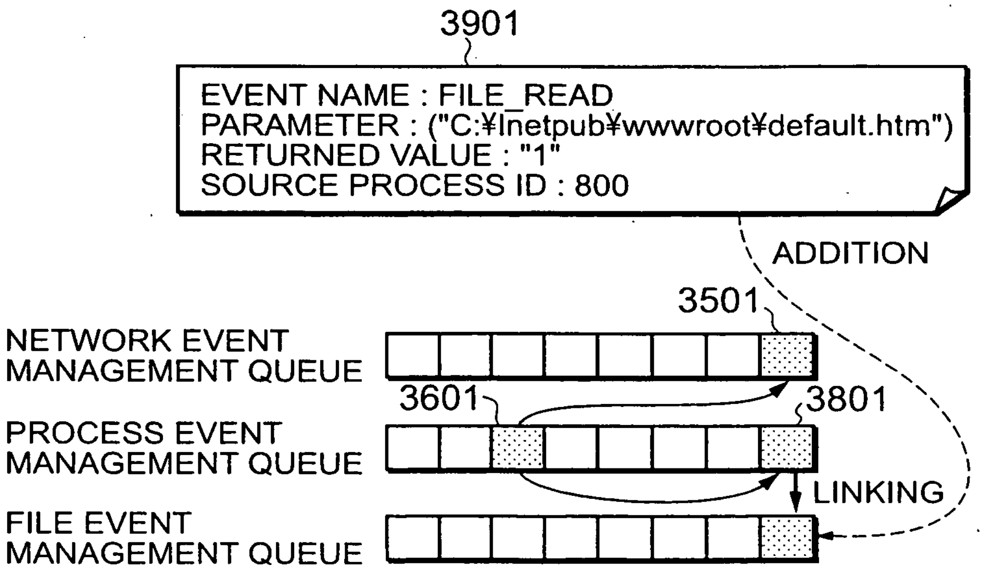

3901
EVENT NAME : FILE_READ
PARAMETER : ("C:¥Inetpub¥wwwroot¥default.htm")
RETURNED VALUE : "1"
SOURCE PROCESS ID : 800
ADDITION
3501
NETWORK EVENT MANAGEMENT QUEUE
3601
3801
PROCESS EVENT MANAGEMENT QUEUE
LINKING
FILE EVENT MANAGEMENT QUEUE

FIG. 46

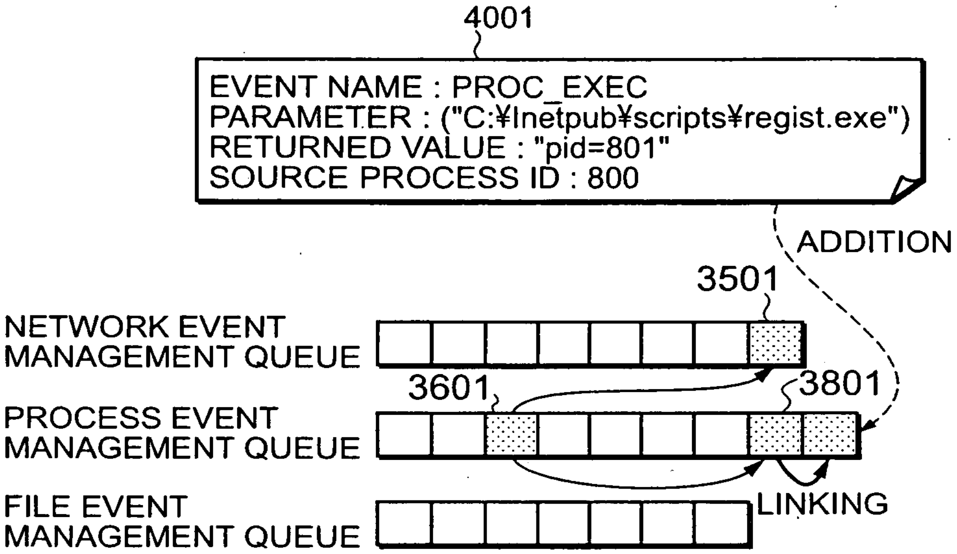

4001
EVENT NAME : PROC_EXEC
PARAMETER : ("C:¥Inetpub¥scripts¥regist.exe")
RETURNED VALUE : "pid=801"
SOURCE PROCESS ID : 800
ADDITION
3501
NETWORK EVENT MANAGEMENT QUEUE
3601
3801
PROCESS EVENT MANAGEMENT QUEUE
LINKING
FILE EVENT MANAGEMENT QUEUE

FIG. 47

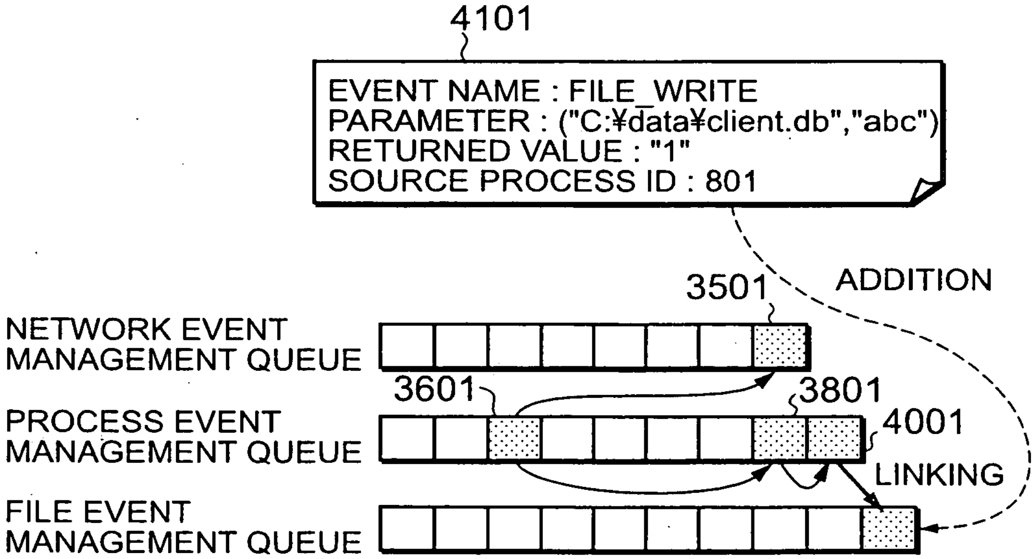
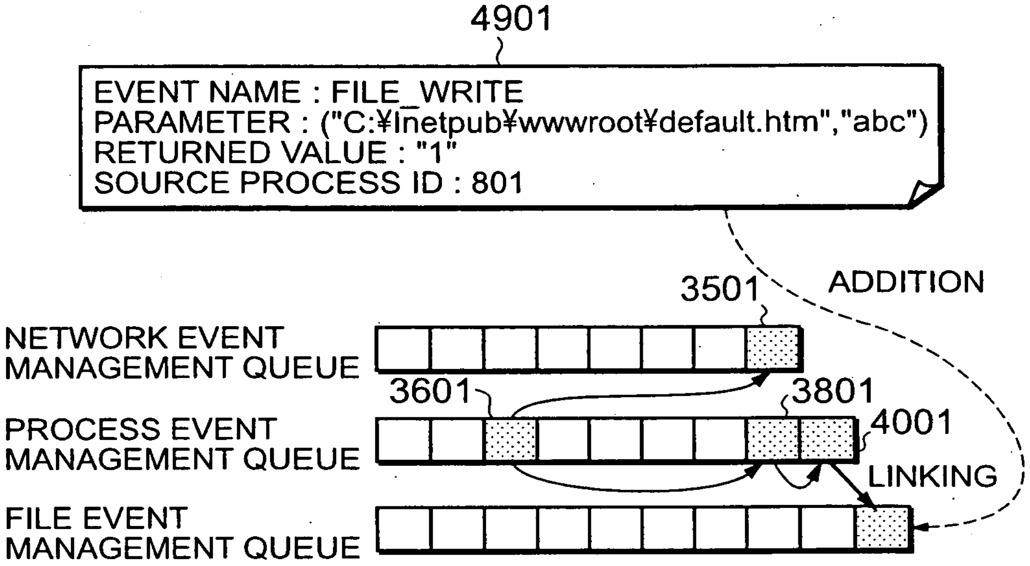

4101
EVENT NAME : FILE_WRITE
PARAMETER : ("C:¥data¥client.db","abc")
RETURNED VALUE : "1"
SOURCE PROCESS ID : 801
ADDITION
3501
NETWORK EVENT MANAGEMENT QUEUE
3601
3801
4001
PROCESS EVENT MANAGEMENT QUEUE
LINKING
FILE EVENT MANAGEMENT QUEUE

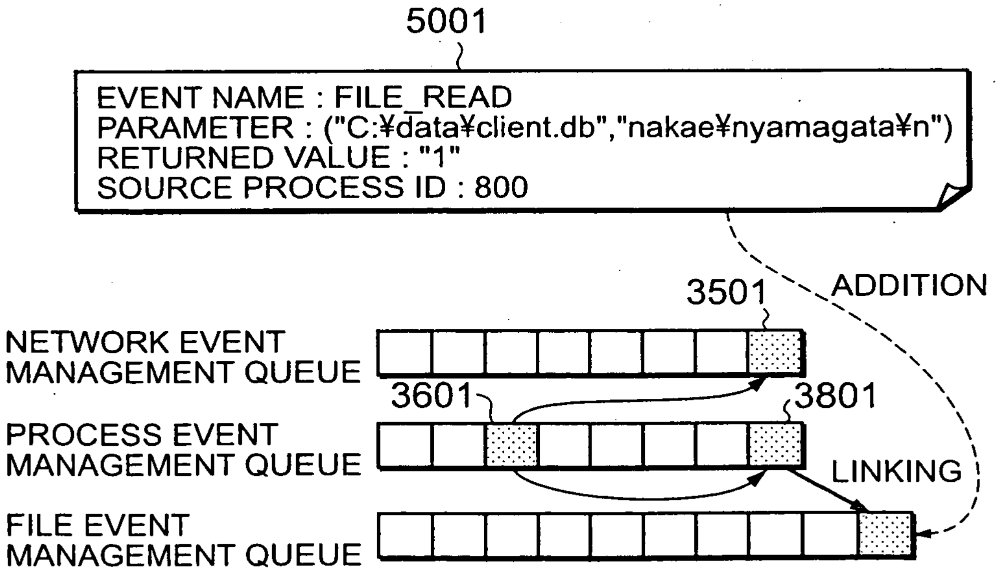
FIG. 48



EVENT NAME : FILE_WRITE
PARAMETER : ("C:¥Inetpub¥wwwroot¥default.htm","abc")
RETURNED VALUE : "1"
SOURCE PROCESS ID : 801

4901
ADDITION
3501
NETWORK EVENT MANAGEMENT QUEUE
3601
3801
4001
PROCESS EVENT MANAGEMENT QUEUE
LINKING
FILE EVENT MANAGEMENT QUEUE

FIG. 49



EVENT NAME : FILE_READ
PARAMETER : ("C:¥data¥client.db","nakae¥nyamagata¥n")
RETURNED VALUE : "1"
SOURCE PROCESS ID : 800

5001
ADDITION
3501
NETWORK EVENT MANAGEMENT QUEUE
3601
3801
PROCESS EVENT MANAGEMENT QUEUE
LINKING
FILE EVENT MANAGEMENT QUEUE

FIG. 50

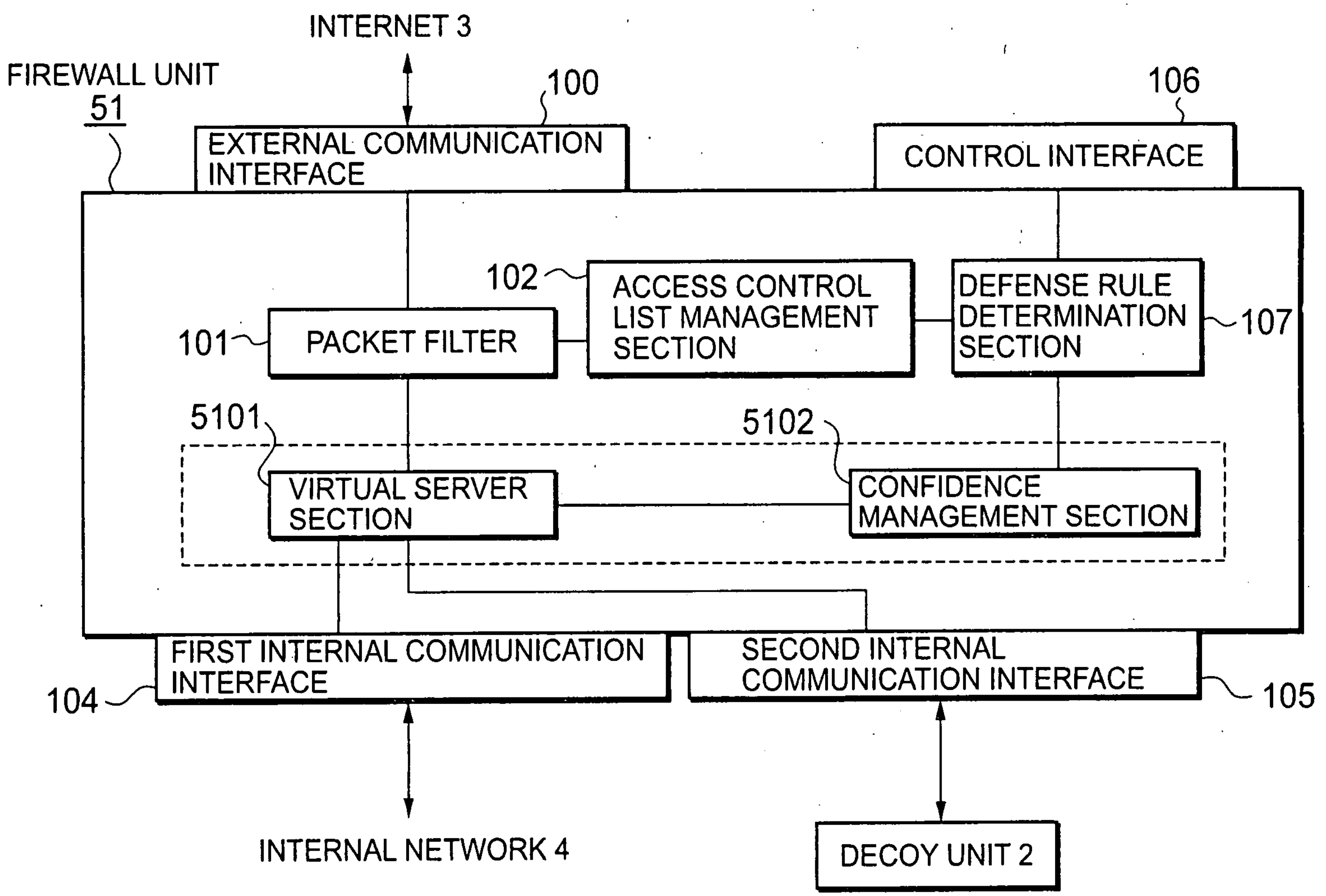

INTERNET 3
FIREWALL UNIT
51
100
EXTERNAL COMMUNICATION INTERFACE
106
CONTROL INTERFACE
102
ACCESS CONTROL LIST MANAGEMENT SECTION
DEFENSE RULE DETERMINATION SECTION
107
101
PACKET FILTER
5101
5102
VIRTUAL SERVER SECTION
CONFIDENCE MANAGEMENT SECTION
FIRST INTERNAL COMMUNICATION INTERFACE
SECOND INTERNAL COMMUNICATION INTERFACE
104
105
INTERNAL NETWORK 4
DECOY UNIT 2

FIG. 51

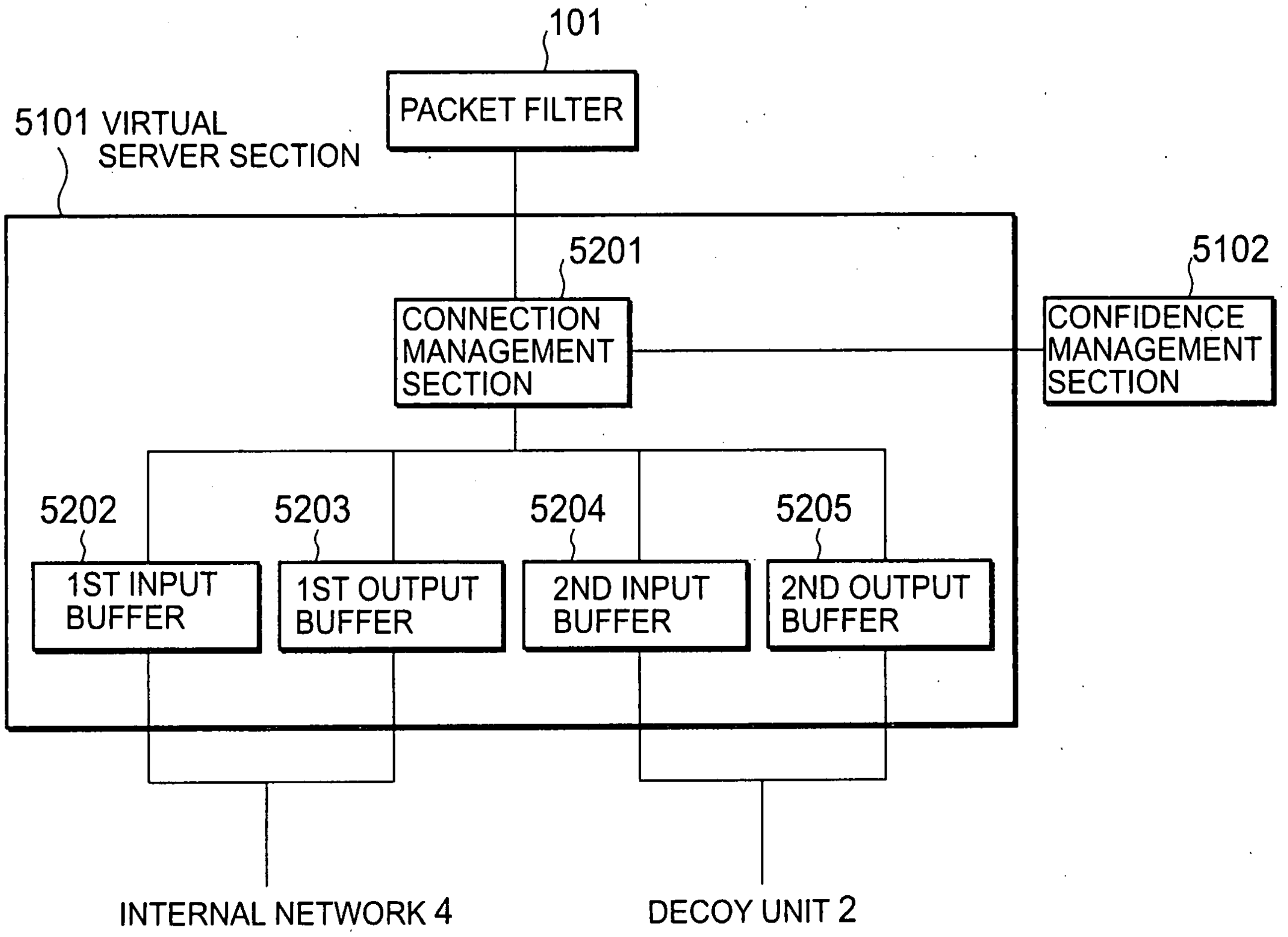

101
PACKET FILTER
5101 VIRTUAL SERVER SECTION
5201
CONNECTION MANAGEMENT SECTION
5102
CONFIDENCE MANAGEMENT SECTION
5202
1ST INPUT BUFFER
5203
1ST OUTPUT BUFFER
5204
2ND INPUT BUFFER
5205
2ND OUTPUT BUFFER
INTERNAL NETWORK 4
DECOY UNIT 2

FIG. 52

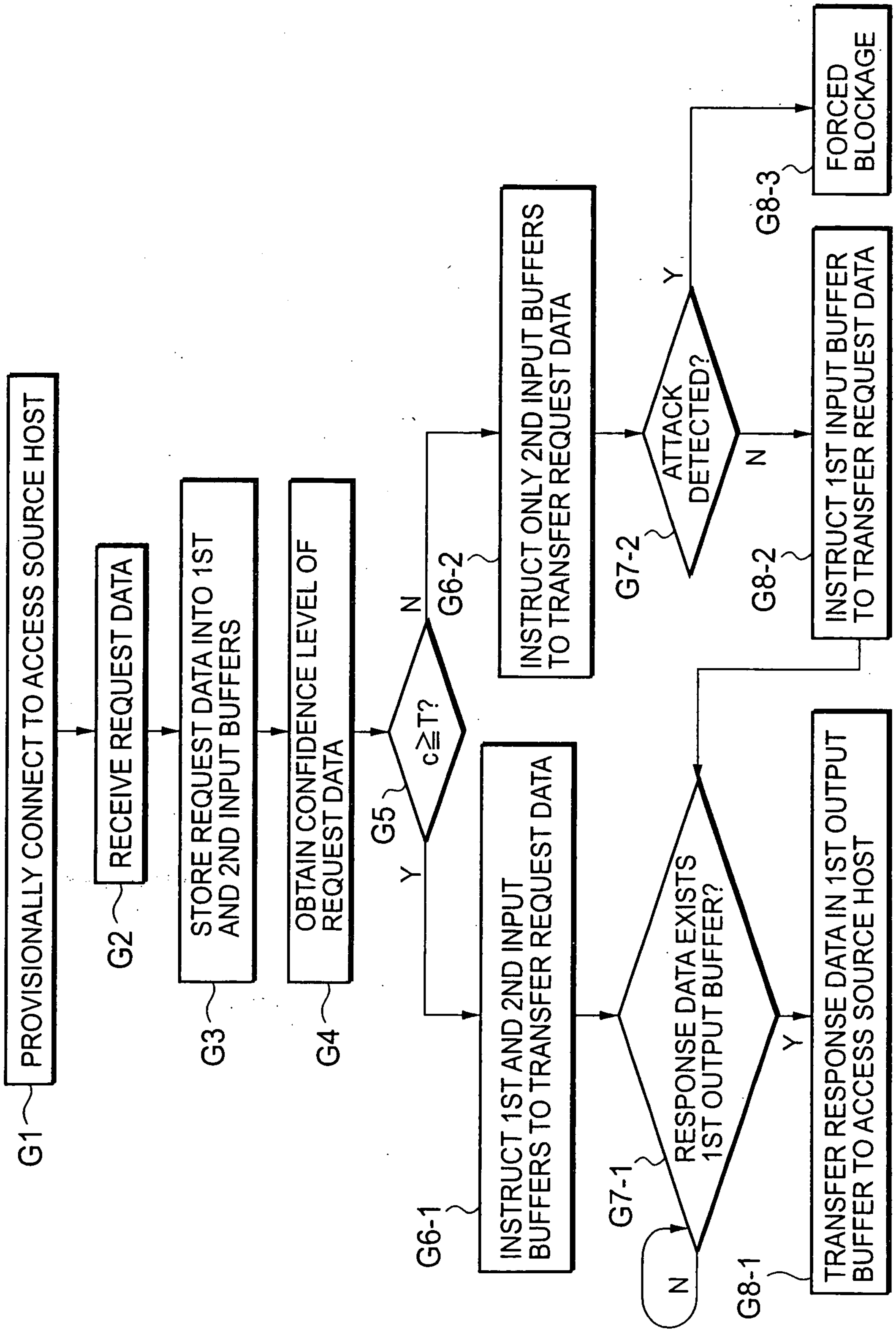

G1
PROVISIONALLY CONNECT TO ACCESS SOURCE HOST
G2
RECEIVE REQUEST DATA
G3
STORE REQUEST DATA INTO 1ST AND 2ND INPUT BUFFERS
G4
OBTAIN CONFIDENCE LEVEL OF REQUEST DATA
G5
c≧T?
Y
N
G6-1
INSTRUCT 1ST AND 2ND INPUT BUFFERS TO TRANSFER REQUEST DATA
G6-2
INSTRUCT ONLY 2ND INPUT BUFFERS TO TRANSFER REQUEST DATA
G7-1
RESPONSE DATA EXISTS 1ST OUTPUT BUFFER?
N
Y
G7-2
ATTACK DETECTED?
N
Y
G8-1
TRANSFER RESPONSE DATA IN 1ST OUTPUT BUFFER TO ACCESS SOURCE HOST
G8-2
INSTRUCT 1ST INPUT BUFFER TO TRANSFER REQUEST DATA
G8-3
FORCED BLOCKAGE

FIG. 53

REQUEST DATA	CONFIDENCE LEVEL
D0	1
D1	0
. . .	. . .
Dn	1

FIG. 54

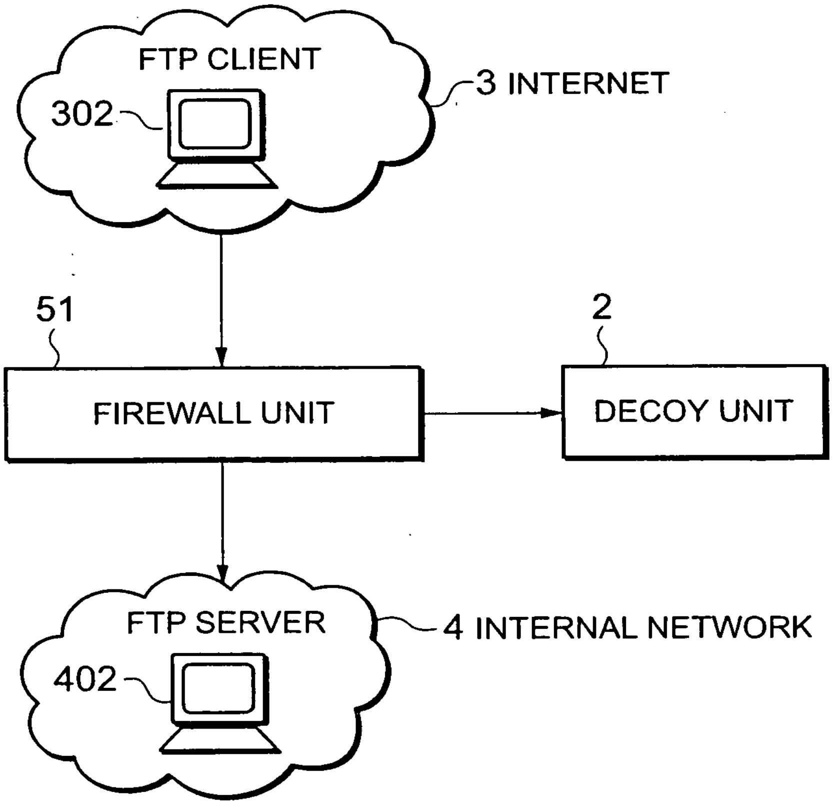


FIG. 55

REQUEST DATA	CONFIDENCE LEVEL
D0	1
D1	0
· · ·	· · ·
1	0

FIG. 56

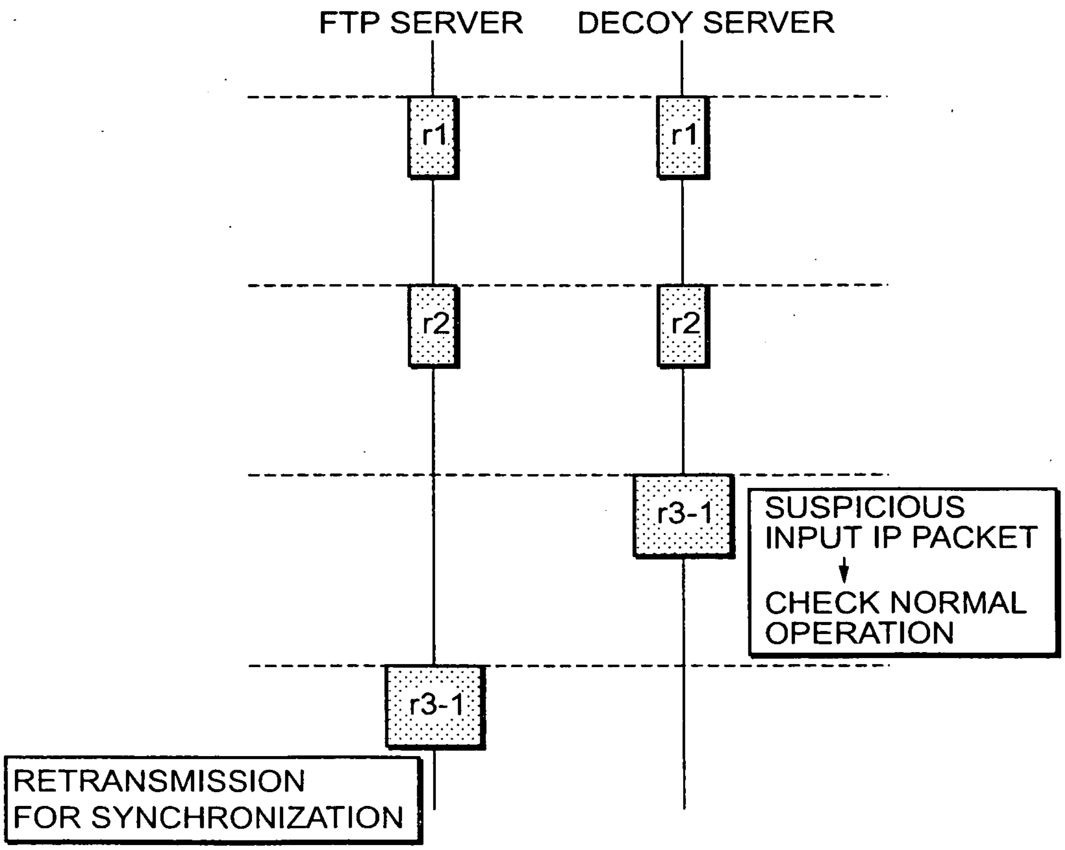

FTP SERVER
DECOY SERVER
r1
r1
r2
r2
r3-1
SUSPICIOUS INPUT IP PACKET
CHECK NORMAL OPERATION
r3-1
RETRANSMISSION FOR SYNCHRONIZATION

FIG. 57

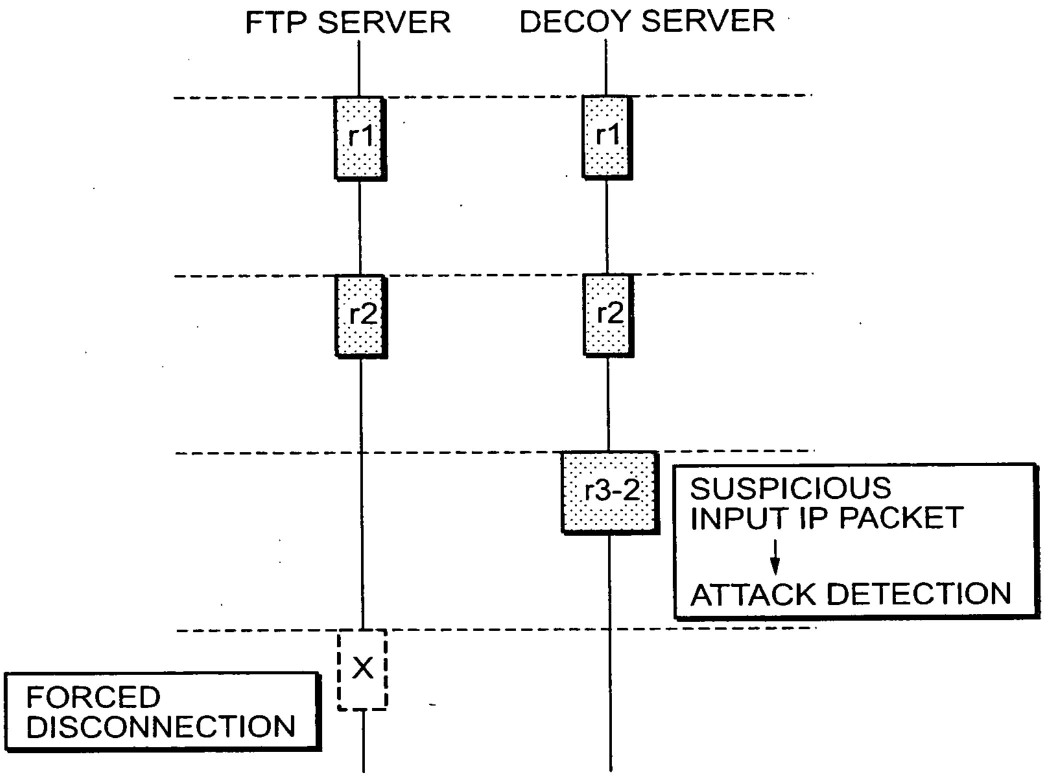

FTP SERVER
DECOY SERVER
r1
r1
r2
r2
r3-2
SUSPICIOUS INPUT IP PACKET
ATTACK DETECTION
X
FORCED DISCONNECTION

FIG. 58

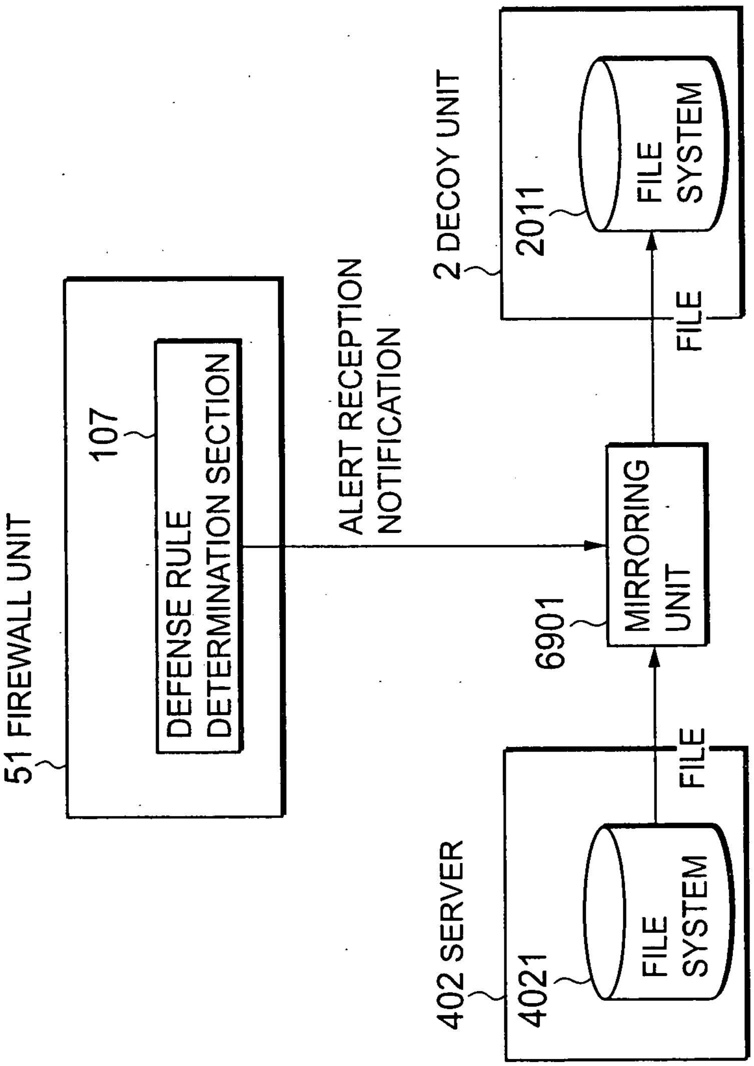

51 FIREWALL UNIT
107
DEFENSE RULE DETERMINATION SECTION
ALERT RECEPTION NOTIFICATION
402 SERVER
4021
FILE SYSTEM
FILE
6901
MIRRORING UNIT
FILE
2 DECOY UNIT
2011
FILE SYSTEM

FIG. 59

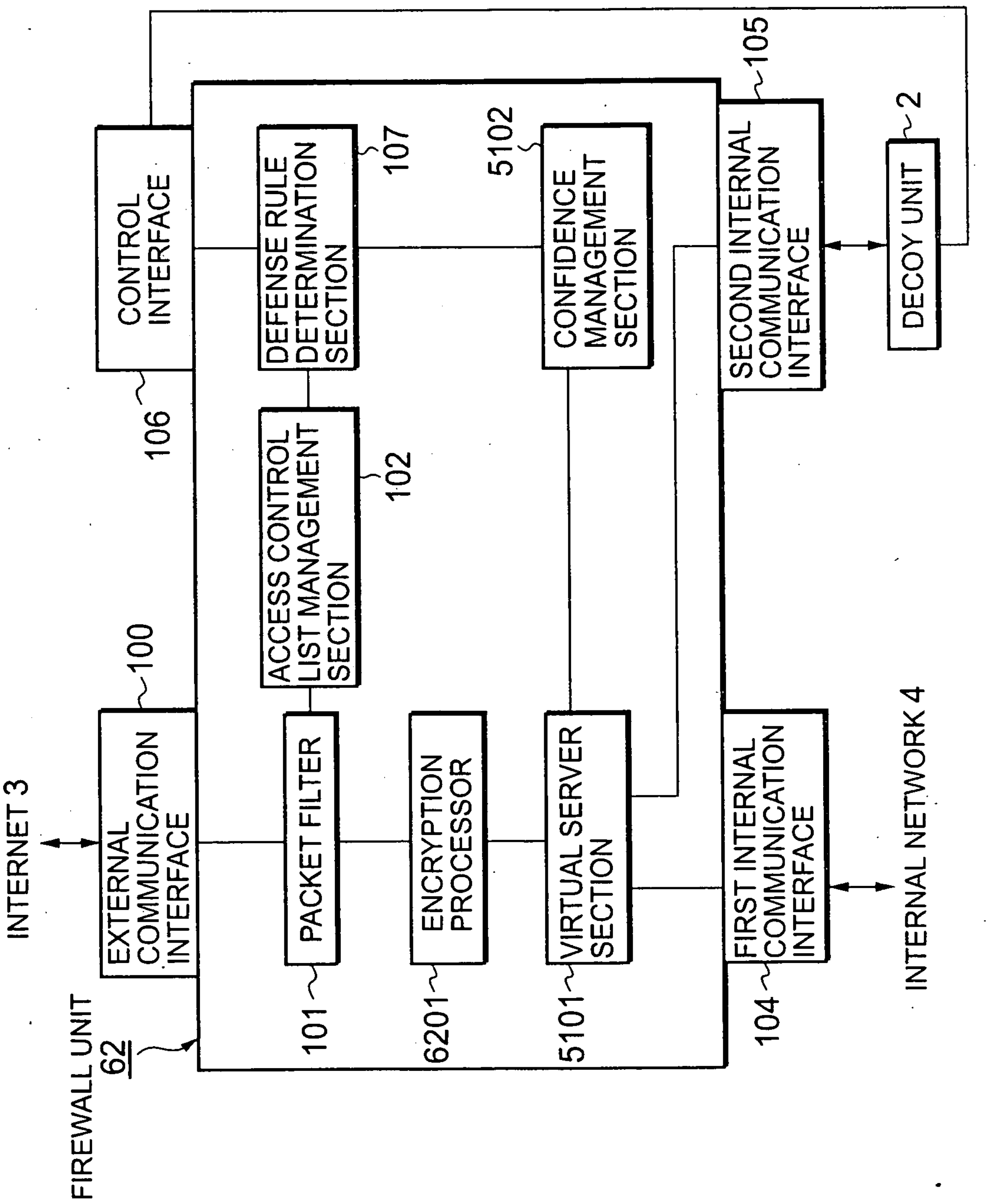

INTERNET 3
EXTERNAL COMMUNICATION INTERFACE
100
FIREWALL UNIT 62
PACKET FILTER
101
ENCRYPTION PROCESSOR
6201
VIRTUAL SERVER SECTION
5101
FIRST INTERNAL COMMUNICATION INTERFACE
104
INTERNAL NETWORK 4
CONTROL INTERFACE
106
DEFENSE RULE DETERMINATION SECTION
107
ACCESS CONTROL LIST MANAGEMENT SECTION
102
CONFIDENCE MANAGEMENT SECTION
5102
SECOND INTERNAL COMMUNICATION INTERFACE
105
DECOY UNIT
2

FIG. 60

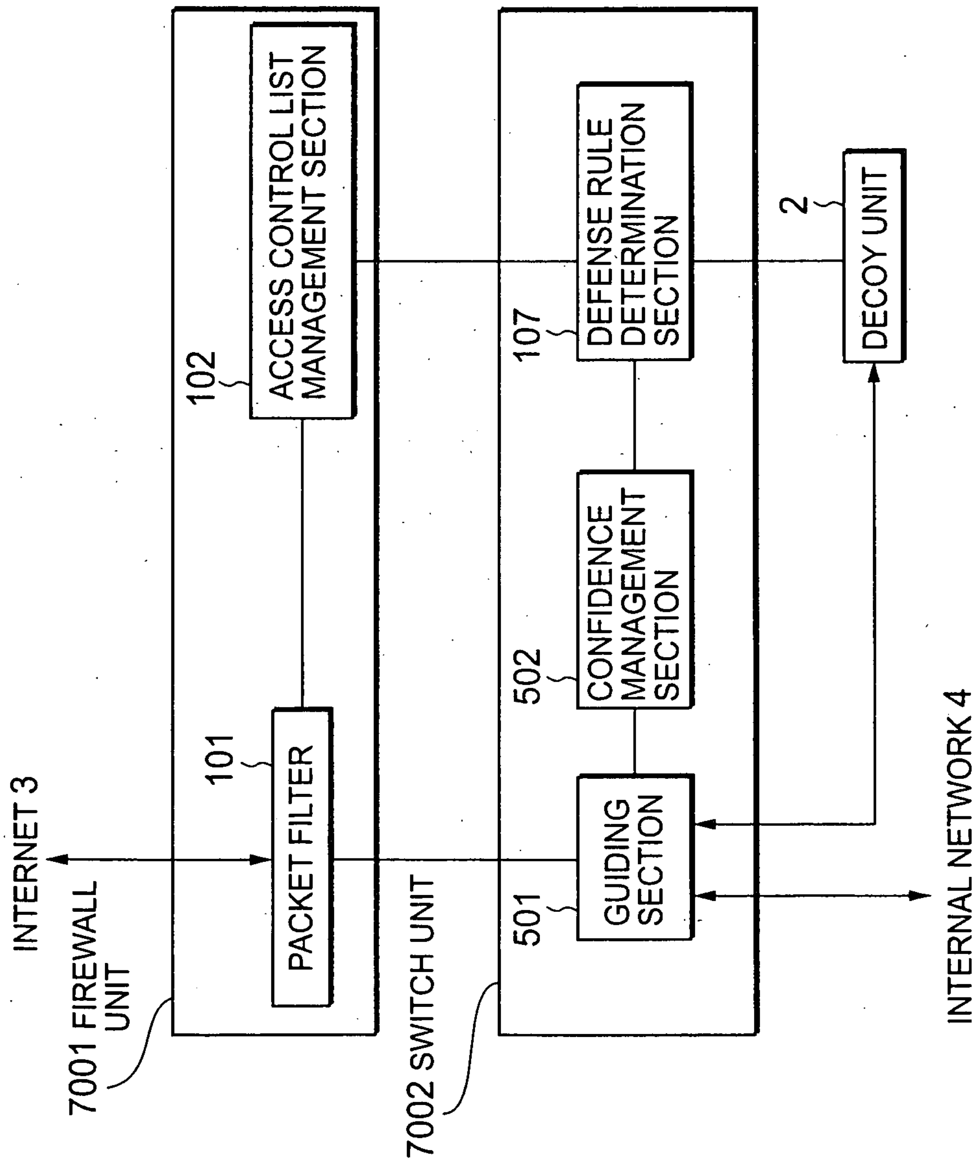

INTERNET 3
7001 FIREWALL UNIT
101
PACKET FILTER
102
ACCESS CONTROL LIST MANAGEMENT SECTION
7002 SWITCH UNIT
501
GUIDING SECTION
502
CONFIDENCE MANAGEMENT SECTION
107
DEFENSE RULE DETERMINATION SECTION
2
DECOY UNIT
INTERNAL NETWORK 4

FIG. 61

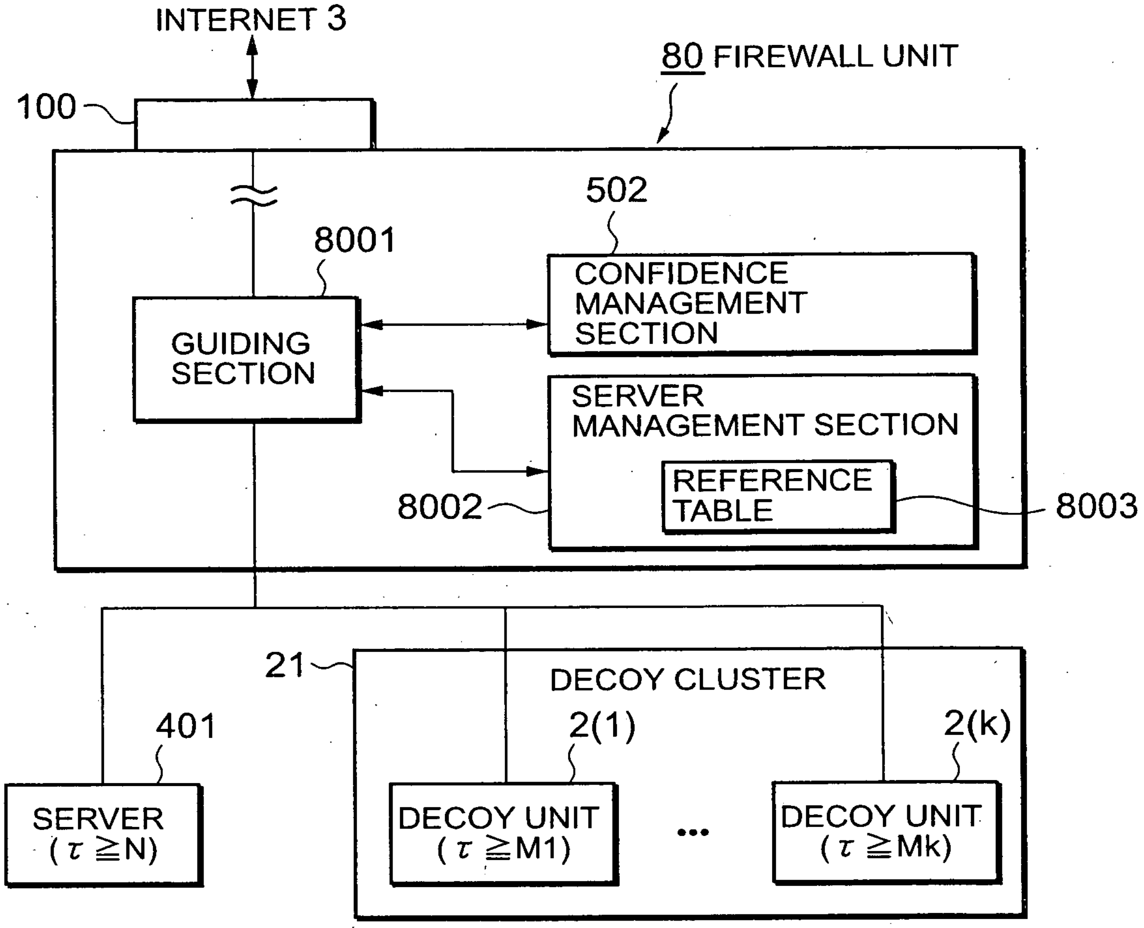


FIG. 62

8003 REFERENCE TABLE

SERVER IDENTIFIER	REQUISITE CONFIDENCE LEVEL
D1	M1
D2	M2
. . .	. . .
Dk	Mk

FIG. 63

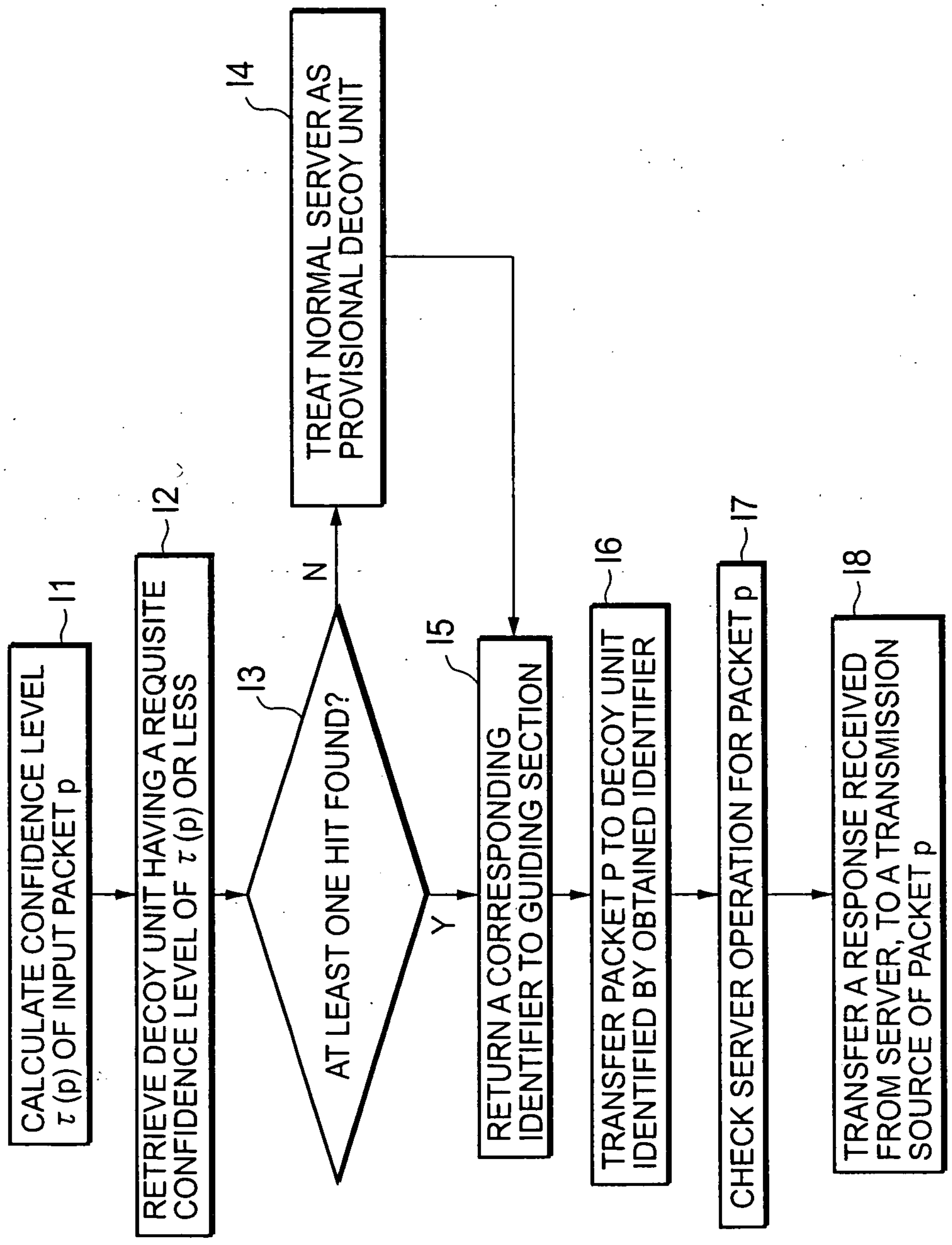

I1
CALCULATE CONFIDENCE LEVEL τ (p) OF INPUT PACKET p
I2
RETRIEVE DECOY UNIT HAVING A REQUISITE CONFIDENCE LEVEL OF τ (p) OR LESS
I3
AT LEAST ONE HIT FOUND?
N
Y
I4
TREAT NORMAL SERVER AS PROVISIONAL DECOY UNIT
I5
RETURN A CORRESPONDING IDENTIFIER TO GUIDING SECTION
I6
TRANSFER PACKET P TO DECOY UNIT IDENTIFIED BY OBTAINED IDENTIFIER
I7
CHECK SERVER OPERATION FOR PACKET p
I8
TRANSFER A RESPONSE RECEIVED FROM SERVER, TO A TRANSMISSION SOURCE OF PACKET p

FIG. 64

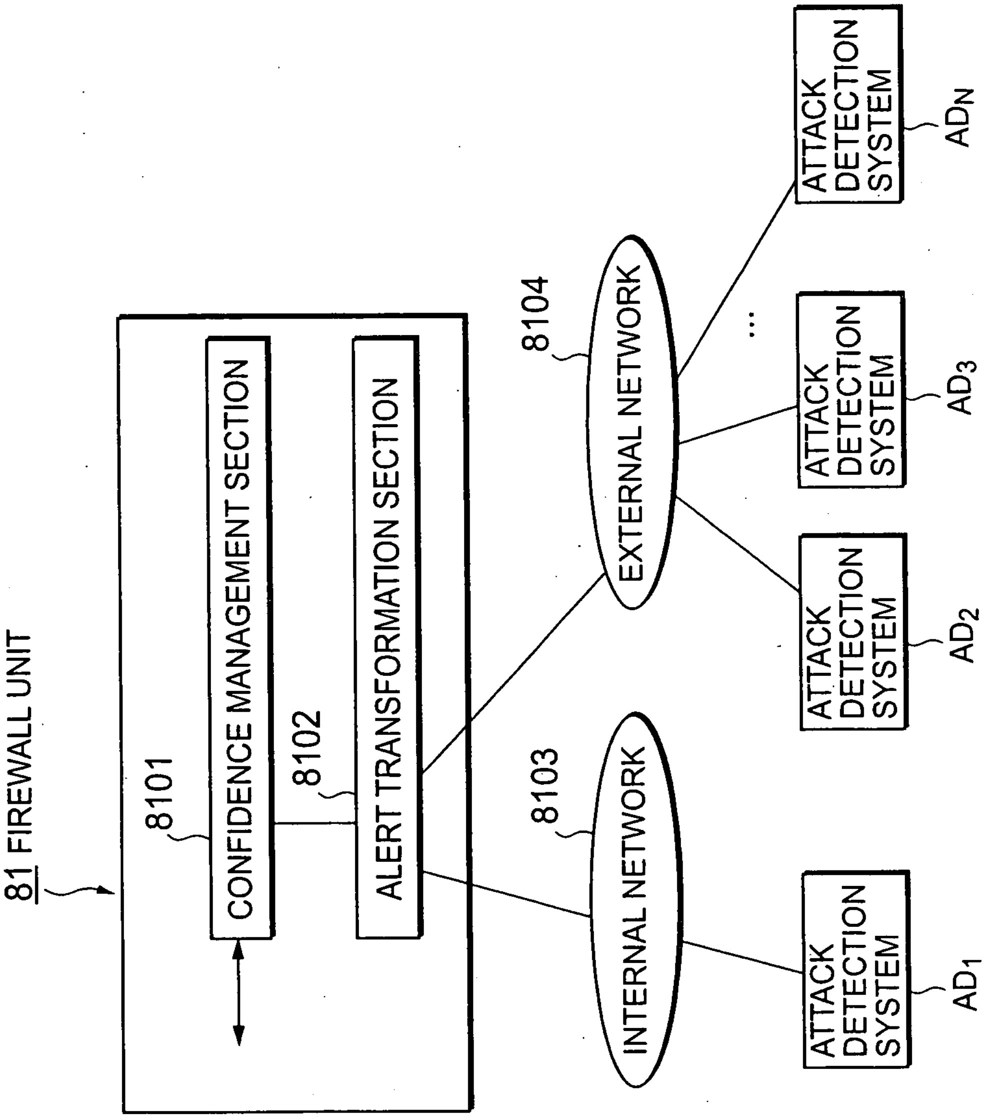

81 FIREWALL UNIT
8101
CONFIDENCE MANAGEMENT SECTION
8102
ALERT TRANSFORMATION SECTION
8103
INTERNAL NETWORK
8104
EXTERNAL NETWORK
ATTACK DETECTION SYSTEM
AD_1
ATTACK DETECTION SYSTEM
AD_2
ATTACK DETECTION SYSTEM
AD_3
...
ATTACK DETECTION SYSTEM
AD_N

FIG. 65

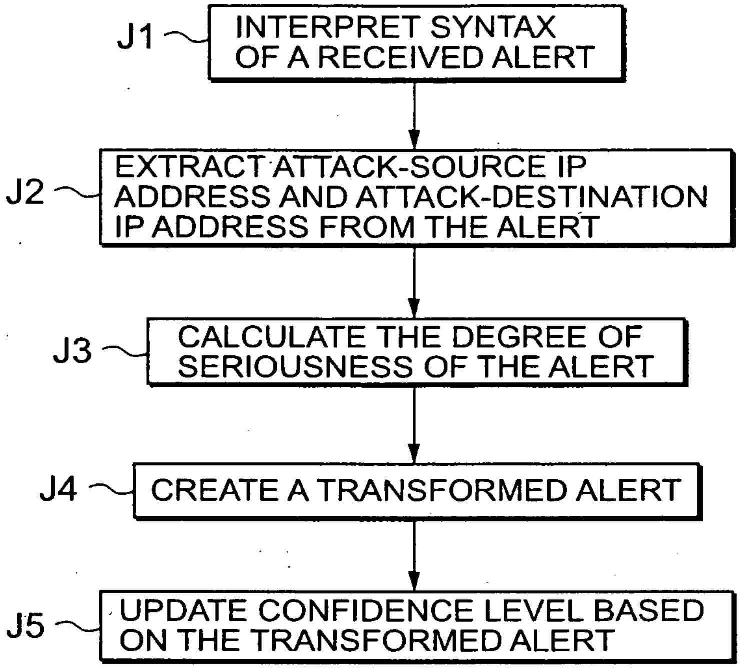

J1
INTERPRET SYNTAX OF A RECEIVED ALERT
J2
EXTRACT ATTACK-SOURCE IP ADDRESS AND ATTACK-DESTINATION IP ADDRESS FROM THE ALERT
J3
CALCULATE THE DEGREE OF SERIOUSNESS OF THE ALERT
J4
CREATE A TRANSFORMED ALERT
J5
UPDATE CONFIDENCE LEVEL BASED ON THE TRANSFORMED ALERT

FIG. 66

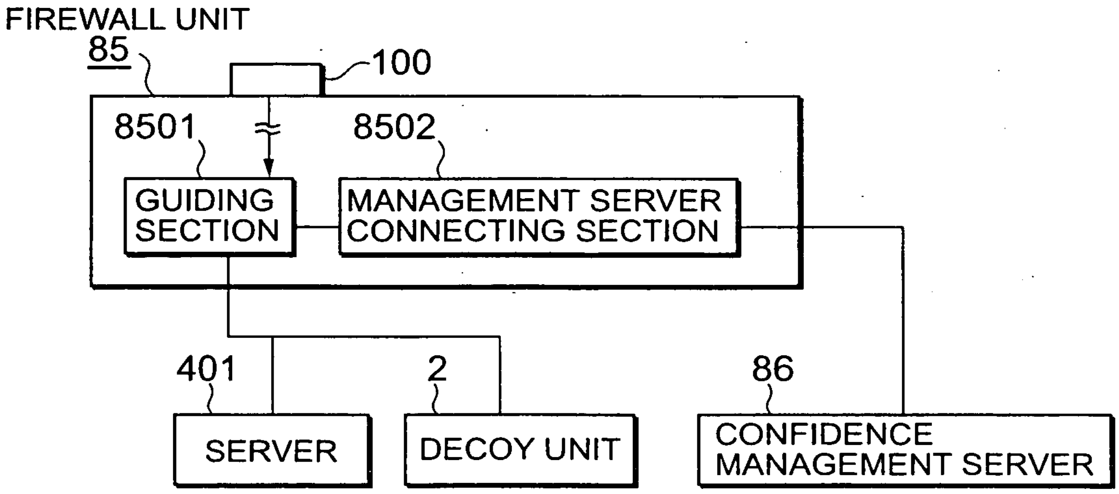
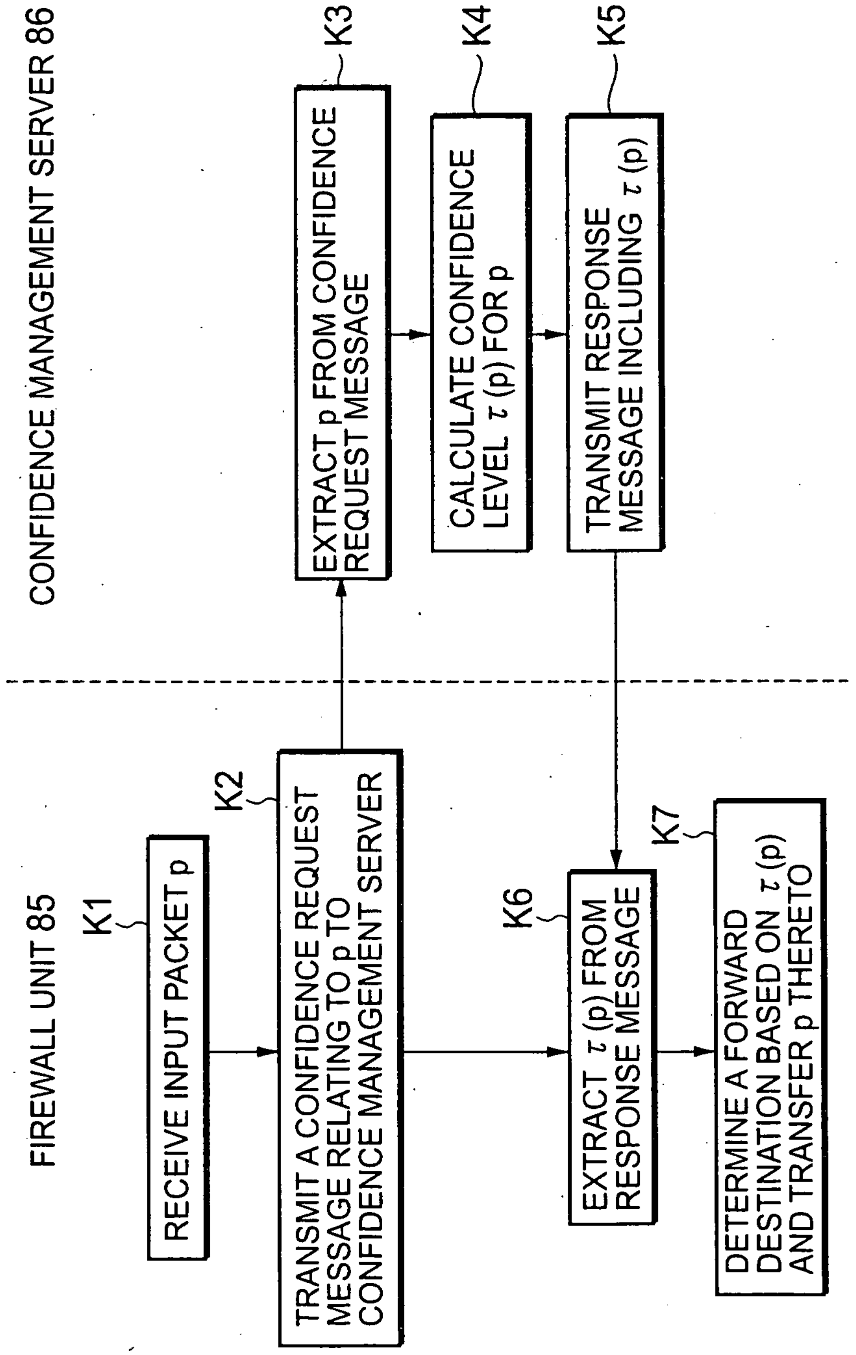

FIREWALL UNIT
85
100
8501
GUIDING SECTION
8502
MANAGEMENT SERVER CONNECTING SECTION
401
SERVER
2
DECOY UNIT
86
CONFIDENCE MANAGEMENT SERVER

FIG. 67


FIREWALL UNIT 85
CONFIDENCE MANAGEMENT SERVER 86
K1
RECEIVE INPUT PACKET p
K2
TRANSMIT A CONFIDENCE REQUEST MESSAGE RELATING TO p TO CONFIDENCE MANAGEMENT SERVER
K3
EXTRACT p FROM CONFIDENCE REQUEST MESSAGE
K4
CALCULATE CONFIDENCE LEVEL τ (p) FOR p
K5
TRANSMIT RESPONSE MESSAGE INCLUDING τ (p)
K6
EXTRACT τ (p) FROM RESPONSE MESSAGE
K7
DETERMINE A FORWARD DESTINATION BASED ON τ (p) AND TRANSFER p THERETO